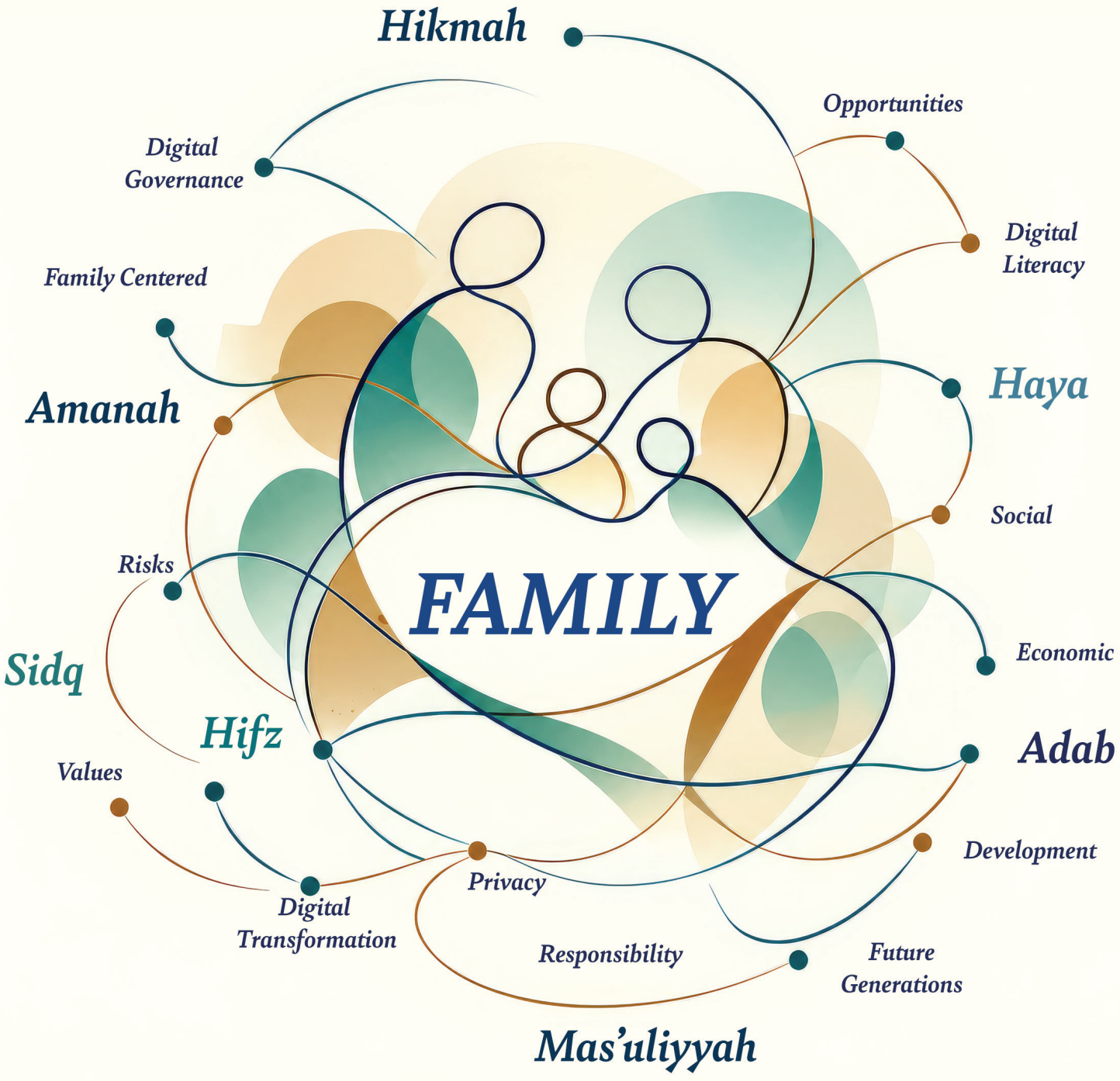
COMCEC

Digital Threats to Family Institution as Backbone of Development and Value-Based Solutions



November 2026

Standing Committee
for Economic and Commercial Cooperation of the
Organization of the Islamic Cooperation

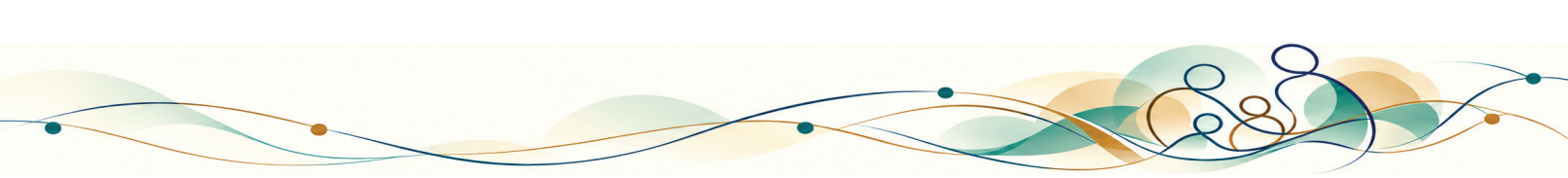
COMCEC

DIGITAL THREATS TO FAMILY INSTITUTION AS BACKBONE OF DEVELOPMENT AND VALUE-BASED SOLUTIONS

COMCEC COORDINATION OFFICE

Ankara, Türkiye
October 2026





COMCEC

This report has been commissioned by the Committee for Economic and Commercial Cooperation of the Organization of Islamic Cooperation (COMCEC) Coordination Office and prepared by a team led by Prof. Dr. H. Ferhan ODABAŞI, comprising academics and experts from the COMCEC Coordination Office (CCO), including Aylin ŞENOL GÜN (Senior Expert), Mine DEMİR (Expert), and Ç. İrem KAYA (Expert).The opinions expressed in the report are solely those of the authors and do not represent the official views of the CCO or the Member Countries of the Organization of Islamic Cooperation (OIC). The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the COMCEC/CCO concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its political regime or frontiers or boundaries. Designations such as "developed," "developing," "emerging," "low-income", etc. Are intended for statistical convenience and do not necessarily express a judgement about the state reached by a particular country or area in the development process. The mention of firm names or commercial products does not imply endorsement by COMCEC and/or CCO. The final version of the report is available at the COMCEC website. Excerpts from the report can be made as long as references are provided. All intellectual and industrial property rights for the report belong to the CCO. This report is for individual use and it shall not be used for commercial purposes. Except for purposes of individual use, this report shall not be reproduced in any form or by any means, electronic or mechanical, including printing, photocopying, CD recording, or by any physical or electronic reproduction system, or translated and provided to the access of any subscriber through electronic means for commercial purposes without the permission of the CCO.

TABLE OF CONTENTS

LIST OF FIGURES iii

LIST OF TABLES iv

LIST OF ACRONYMS v

GLOSSARY viii

EXECUTIVE SUMMARY 1

INTRODUCTION 3

1. CONCEPTUAL AND ANALYTICAL FRAMEWORK: FAMILY INSTITUTION AND ITS ISLAMIC VALUE FOUNDATIONS 5

1.1. Family as a Social and Civilizational Institution 5

1.2. Family as the Backbone of Development 5

1.3. Family in Islamic Civilization 6

1.4. Understanding Digital Family Governance 8

1.5. Viewing Digital Family Governance Through Core Islamic Principles 9

2. DIGITALIZATION AND THE CHANGING NATURE OF FAMILY 17

2.1. Conceptualizing the Digitalization of Family Life 17

2.2. Digital Opportunities for Family and Child Well-Being 19

2.3. Digital Risks to Family Integrity, Socialization and Values 20

2.4. Transformation of Family Values in Digital Environments 23

3. TRENDS IN FAMILY AND DIGITAL GOVERNANCE: GLOBAL AND OIC PERSPECTIVES 31

3.1. Global Context in Brief: Evolution of Digital Family Governance 31

3.2. Emerging Trends in Family and Child-Centered Digital Governance 33

3.3. Evolution of Regulatory Framework: Global Approaches and OIC Practices 34

3.4. Models of Institutional Governance: Structures and Coordination 38

3.5. Implementation Mechanisms and Policy Instruments 41

3.6. Patterns, Gaps, and Emerging Policy Challenges in the OIC Member Countries 43

4. SELECTED COUNTRY CASE STUDIES: POLICY APPROACHES AND GOOD PRACTICES IN DIGITAL FAMILY GOVERNANCE 46

4.1. TÜRKİYE 46
4.1.1. Introduction 46
4.1.2. Policy and Regulatory Framework 51
4.1.3. Institutional Structure and Governance 70
4.1.4. Implementation Mechanisms and Policy Instruments 73
4.1.5. Challenges, Areas for Improvement and Key Takeaways 75
4.1.6. Lessons Learned from Effective Practices 76

4.2. MALAYSIA 77
4.2.1. Introduction 77
4.2.2. Regulatory Framework 80
4.2.3. Institutional Governance Structure 85
4.2.4. Implementation Mechanisms and Policy Instruments 90
4.2.5. Implementation Challenges and Areas for Further Strengthening 101
4.2.6. Lessons Learned 101

4.3. JORDAN 102
4.3.1. Introduction 102
4.3.2. Regulatory Framework 106
4.3.3. Institutional Governance Structure 110
4.3.4. Implementation Mechanisms and Policy Instruments 112
4.3.5. Lessons Learned Error! Bookmark not defined 117

4.4. NIGERIA 117
4.4.1. Introduction 117
4.4.2. Regulatory Framework 121
4.4.3. Institutional Governance Structure 123
4.4.4. Implementation Mechanisms and Policy Instruments 124
4.4.5. Lessons Learned 125

4.5. HUNGARY 126
4.5.1. Introduction 126
4.5.2. Regulatory Framework 128
4.5.3. Institutional Governance Structure 131
4.5.4. Implementation Mechanisms and Policy Instruments 133
4.5.5. Lessons Learned 135

5. CONCLUSION AND POLICY RECOMMENDATIONS 137

REFERENCES 145

LIST OF FIGURES

Figure 2.1 Parental mediation strategies 20

Figure 2.2 Factors Affecting the Digitalization of the Family 24

Figure 3.1 Selected Connectivity Indicators: OIC and World, 2023 33

Figure 3.2 Centralized Governance Model 39

Figure 3.3 Decentralized Governance Model 40

Figure 4.1 Scope of the Vision Document and Action Plan for the Protection and Strengthening of the Family 53

Figure 4.2 Stakeholders of the Vision Document and Action Plan for the Protection and Strengthening of the Family 54

Figure 4.3 Stakeholders of the Action Plan for Empowering Children in the Digital World 57

Figure 4.4 Strategic Objectives of the Action Plan for the Empowerment of Children in the Digital World (2026–2030) 58

Figure 4.5 Digital Child Protection Policy Cycle 60

Figure 4.6 Institutional Governance Framework for the Protection of Children and Families in the Digital Environment in Türkiye 71

Figure 4.7 Number of Internet Users in Malaysia (million) 77

Figure 4.8 Individuals Using the Internet in Nigeria, 2020–2024 118

Figure 4.9 Individuals Using the Internet in Hungary, 2020–2024 127

LIST OF TABLES

Table 1.1 Complementary Roles of Hikmah and Mas'uliyyah in Digital Family Governance 15

Table 1.2 Applying Islamic Values through Hikmah and Mas'uliyyah 16

Table 2.1 Risks for Children in the Digital Environment 20

Table 2.2 Main Digital Opportunities and Risks for Family and Child Well-Being from a Value-Based Perspective 23

Table 2.3 Illustrative Value-Based Framework for Digital Family Policies and Services 30

Table 3.1 Global Regulatory Approaches and Implications for the OIC Context 38

Table 3.2 OIC Member Countries by GTMI Groups, 2025 44

Table 4.1 Key Indicators on Family and Population Transformation 47

Table 4.2 Internet Use by Age Group 47

Table 4.3 Daily Screen Use of Six Hours or More 48

Table 4.4 Selected Indicators of Digital Use, Daily Routines and Social Relationships 48

Table 4.5 Key National Policy Documents Relevant to Digital Family Governance 52

Table 4.6 Responsible Institutions and Selected Activities for Supporting the Family in the Process of Digitalization 55

Table 4.7 Strategic Targets, Responsible Institutions and Activities under "Access to Information Technologies and Safe Internet Use" 59

Table 4.8 Key Legislative Framework Relevant to Digital Family Governance in Türkiye 61

Table 4.9 Selected Educational, Guidance and Information Tools for Families and Children 66

Table 4.10 Selected TRT Digital Initiatives for Children and Families 67

Table 4.11 Selected RTÜK Media Literacy and Awareness Tools for Children and Families 68

Table 4.12 Selected Practices Supporting Digital Family Governance in Türkiye 73

Table 4.13 The KASIH Framework of the National Family Compassion Policy 81

Table 4.14 Malaysia's National Policy and Legislative Framework for Families and Digital Transformation 85

Table 4.15 Institutional Architecture of Digital Governance in Malaysia: Key Institutions by Functional Level 90

Table 4.16 KDB Key Performance Indicators (2012-2024) 95

Table 4.17 Key Elements of Platform KID's Content Development Approach 98

Table 4.18 Key Dimensions of Platform KID's Value-Based Approach to Digital Parenting 99

Table 4.19 A Comparative Analysis of Digital Family Governance Initiatives in Malaysia 100

Table 4.20 Jordan's Policy and Legislative Framework Relevant to Digital Family Governance 108

Table 4.21 Institutional Architecture of Digital Family Governance in Jordan 111

Table 4.22 Comparative Analysis of Digital Family-Governance Tools in Jordan 114

Table 4.23 Selected Practices and Key Features of Digital Family Governance in Jordan 116

Table 4.24 Key Demographic and Digital Indicators for Nigeria 120

Table 4.25 Selected Findings on Families and Digitalization in Hungary 128

Table 4.26 Regulatory and Policy Framework for Digital Family Governance in Hungary 130

Table 4.27 Institutional Architecture of Digital Family Governance in Hungary 133

LIST OF ACRONYMS

3MTT:	3 Million Technical Talent
ACSAI:	Action Against Child Sexual Abuse Initiative
AI:	Artificial Intelligence
API:	Application Programming Interface
BIK:	Better Internet for Kids
BRIDGE:	Building Resilient Digital Infrastructure for Growth
BTK:	Information Technologies and Communication Authority
CEB:	Council of Europe Development Bank
CIII:	Digital Citizenship
CMA:	Communication and Multimedia Act
CMRPI:	Moroccan Center for Polytechnic Research and Innovation
COMCEC:	The Standing Committee for Economic and Commercial Cooperation of the Organization of Islamic Cooperation
COP:	Child Online Protection
COPPA:	Children's Online Privacy Protection Act
COVID:	Coronavirus Disease
CRC:	Convention on the Rights of the Child
CSAM:	Child Sexual Abuse Material
CSEA:	Child Sexual Exploitation and Abuse
CSOK:	Family Housing Allowance
DFC:	Digital Family Card
DGYS:	Digital Child Protection Strategy
DigComp:	Digital Competence Framework
DL4ALL:	Digital Literacy for All
DOS:	Digital Education Strategy
DPIA:	Data Protection Impact Assessment
DPO:	Data Protection Officer
DSA:	Digital Services Act
DÁP:	Digital Citizenship Program
EdTech:	Educational Technology
EU:	European Union
FMCIDE:	Federal Ministry of Communications, Innovation and Digital Economy
GDP:	Gross Domestic Product

GDPR:	General Data Protection Regulation
GTMI:	GovTech Maturity Index
HDI:	Human Development Index
HPC:	High-Performance Computing
ICT:	Information and Communication Technology
IMF:	International Monetary Fund
INHOPE:	International Association of Internet Hotlines
IT:	Information Technology
ITU:	International Telecommunication Union
JRF:	Jordan River Foundation
KINCS:	Mária Kopp Institute for Demography and Families
KVKK:	Personal Data Protection Law of Türkiye
MCI:	Ministry of Communications and Information
MDAs:	Ministries, Departments, and Agencies
MoDEE:	Ministry of Digital Economy and Entrepreneurship
MoF:	Ministry of Finance
MoI UAE:	United Arab Emirates Ministry of Interior
NAIRS:	Nigeria Artificial Intelligence Research Scheme
NCAIR:	National Centre for Artificial Intelligence and Robotics
NCC:	Nigerian Communications Commission
NCCM:	National Council for Childhood and Motherhood
NCFA:	National Council for Family Affairs
NCSCM:	National Cyber Security Centre of Jordan
NDEPS:	National Digital Economy Policy and Strategy
NDLF:	National Digital Literacy Framework
NDPA:	Nigeria Data Protection Act
NDPC:	Nigeria Data Protection Commission
NDS:	National Digitalization Strategy
ngCERT:	Nigeria Computer Emergency Response Team
NGO:	Non-Governmental Organization
NGYSZ:	International Children's Safety Service
NHRC:	National Human Rights Commission
NIN:	National Identification Number
NITDA:	National Information Technology Development Agency
NMHH:	National Media and Infocommunications Authority

OECD:	Organisation for Economic Co-operation and Development
OIC:	Organization of Islamic Cooperation
OSA:	Online Safety Act
PDPL:	Personal Data Protection Law
SANAD:	Jordan Digital Government Service
SED:	Socio-economic Status
SESRIC:	Statistical, Economic and Social Research and Training Centre for Islamic Countries
SIC:	Safe Internet Center
SIC+:	Safe Internet Center Plus
SMS:	Short Message Service
SNDGO:	Smart Nation and Digital Government Office
SNPO:	Smart Nation Program Office
STEM:	Science, Technology, Engineering, and Mathematics
TRC:	Telecommunications Regulatory Commission
UAE:	United Arab Emirates
UK:	United Kingdom
UN DESA:	United Nations Department of Economic and Social Affairs
UNDP:	United Nations Development Programme
UNESCO:	United Nations Educational, Scientific and Cultural Organization
UNFPA:	United Nations Population Fund
UNICEF:	United Nations Children's Fund
UNICRI:	United Nations Interregional Crime and Justice Research Institute
WAM:	Emirates News Agency
WB:	World Bank

GLOSSARY

Adab: Ethical conduct and proper behavior that reflect respect, dignity, and good manners in relationships and interactions.

Amanah (Trust): The moral responsibility to fulfil entrusted duties with honesty, integrity, and care.

Amr bil Ma'ruf wa Nahy'an al-Munkar: The Islamic principle of promoting what is right and preventing what is wrong for the benefit of individuals and society.

Cyber Hygiene: The practice of maintaining secure digital habits, such as using strong passwords, updating software, and protecting devices and data from cyber threats.

Digital Family Governance: The ethical, institutional, and relational processes through which families and other societal actors shape the use and governance of digital technologies to protect children, strengthen family well-being, and promote the common good.

Digital Literacy: The ability to access, understand, evaluate, create, and use digital technologies safely, critically, and effectively.

Hifz (Protection): A core normative value in the report's framework encompassing the complementary protection of the family (hifz al-usrah), progeny and future generations (hifz al-nasl), and intellect (hifz al-'aql).

Hifz al-'Aql (Protection of Intellect): A dimension of Hifz concerned with safeguarding human reason, learning, and intellectual well-being.

Hifz al-Nasl (Protection of Progeny/Future Generations): A dimension of Hifz concerned with protecting children, future generations, and the continuity of human well-being.

Hifz al-Usrah (Protection of the Family): A dimension of Hifz concerned with preserving family relationships, stability, and well-being.

Hikmah (Wisdom): The ability to apply knowledge with sound judgement, contextual understanding, and ethical discernment.

Jellyfish Parenting: A highly permissive parenting style characterized by warmth but few rules or boundaries. In digital contexts, it involves limited supervision of children's screen use and online activities.

Maqasid al-Shari'ah: The higher objectives of Islamic law that seek to promote human well-being and protect essential human interests.

Mas'uliyyah (Responsibility): The ethical responsibility to act accountably and fulfil one's obligations according to one's role and capacity.

Media Literacy: The ability to critically access, analyze, evaluate, and interpret media content, including identifying misinformation and assessing the credibility of sources.

Sharenting: The practice of parents or caregivers sharing information, photographs, or videos of their children online, which may affect children's privacy and digital footprint.

Sidq (Truthfulness): Honesty, truthfulness, and integrity in words, actions, and communication.

Wasatiyyah (Moderation): A balanced and proportionate approach that avoids both excess and neglect.

Whole-of-Government Approach: A collaborative approach in which public institutions coordinate policies and actions across sectors to address complex challenges through shared responsibility.

Whole-of-Society Approach: A collaborative approach that engages governments, the private sector, civil society, communities, families, and other stakeholders in addressing complex societal challenges.

EXECUTIVE SUMMARY

Family is a fundamental institution of society. It is where individuals develop a sense of belonging, responsibility and identity, where relationships between generations are formed, and where values, traditions and patterns of care are passed on. Strong family relationships support individual and social well-being and continuity across generations. Through its role in nurturing children, developing human capabilities, providing care and sustaining relationships across generations, the family also contributes to the social and economic foundations of development. In this sense, the family can be regarded as a backbone of development, linking individual well-being and human development with the longer-term development of society. In the OIC Member Countries, family holds a special place in social and cultural life, with family life closely connected to religious values, cultural traditions and the heritage of Islamic civilization.

Families do not exist separately from the environments in which they live. The relationship between family well-being and development works in both directions. Social, economic, cultural and technological changes shape family relationships, everyday practices and families' capacity to provide care as well as support their members. Families, in turn, contribute to the development of human capabilities, the transmission of values and the maintenance of relationships within their communities. Digital technologies, including artificial intelligence (AI), have become an increasingly important part of this interaction, influencing how family members communicate, learn, work, access services and spend time together.

Digital transformation can bring important benefits for families, including wider access to information, education and services, easier communication across distance, and new opportunities for learning, skills development and participation in social and economic life. At the same time, families and children may face risks related to harmful content and contact, cyberbullying, misinformation, privacy, commercial practices and excessive use. Digital technologies can also affect patterns of communication within families, shared time and the ways in which parents guide their children.

In this context, the report examines the implications of digital transformation from a family-centered perspective. It considers not only the protection of children, but also family relationships, parental guidance, the transmission of values and the well-being of future generations. It also recognizes that families cannot address digital challenges on their own. Parents have an important role through communication, guidance, shared rules and role modeling, while governments, technology companies, schools, social services and civil society also have responsibilities in creating safer and more supportive digital environments.

A central part of the report is its consideration of how Islamic values and the intellectual heritage of Islamic civilization can contribute to addressing contemporary digital challenges. The purpose is not to develop a new set of values for the digital age, but to assess how enduring principles can provide useful reference points for family life, public policy and the use of technology.

The report examines digital family life and governance through six core normative values: Amanah (trust and responsible stewardship); Hifz (protection of the family, progeny and intellect); Adab and Haya (ethics, dignity, modesty and privacy); Sidq (truthfulness and integrity); Amr bil- Ma'ruf wa Nahy 'an al-Munkar (promoting good and preventing wrongdoing); and Wasatiyyah (balance and moderation). Two cross-cutting guiding principles, Hikmah (wisdom) and Mas'uliyyah (responsibility and accountability), complement this framework. Together, these concepts provide a value-based lens for considering issues such as family well-being, privacy, responsible behavior, sound judgment, the prevention of harm and the protection of future generations.

The report aims to examine possible connections between enduring values and existing policy approaches. In this way, the values serve as an analytical lens for considering issues such as responsibility, family and child protection, privacy, information integrity, proportionality and context-sensitive judgment, without assuming a direct or explicit connection between particular policies and Islamic principles.

Country case studies from Türkiye, Malaysia, Jordan, Nigeria and Hungary illustrate a range of policy and institutional approaches. They cover areas including digital public services and data protection, digital literacy and awareness, child online safety, parental support, reporting mechanisms and institutional coordination. The cases are not presented as models to be replicated. Rather, they provide examples from different national contexts and help identify practices and lessons that may be relevant to other OIC Member Countries.

Across the cases, the report points to the value of combining different forms of intervention rather than relying on a single measure. Awareness and digital literacy remain important, but they can be supported by accessible reporting, referral, recovery and remedy mechanisms, appropriate safeguards, institutional coordination and monitoring. The appropriate combination will vary according to national contexts, institutional capacities and levels of digital development.

The analysis also suggests scope for greater exchange among the OIC Member Countries. National circumstances differ considerably, and there is no single model of digital family governance that can be applied across all countries. Nevertheless, the importance attached to family life, responsibility, social solidarity and the well-being of future generations provides a basis for sharing experiences, good practices and policy approaches. Cooperation can also support sharing and adaptation of high-quality, culturally relevant digital content and services for families and children across Member Countries, as well as dialogue on common challenges involving global digital platforms.

Based on the analysis and country experiences, the report identifies several areas for policy consideration. These include integrating family-centered and value-based considerations into digital policies; strengthening child and family protection and accountability; improving institutional coordination and strengthening family capacity through practical digital and AI literacy across the life course; making digital inclusion and public services more responsive to family circumstances; and ensuring accessible reporting, referral, recovery, and remedy when harm occurs. The report also emphasizes anticipatory governance for platforms and emerging technologies, stronger OIC-level cooperation, including the sharing and adaptation of safe and culturally relevant digital content and services, and phased implementation supported by outcome-based monitoring.

The report approaches digital transformation not only as a technological development, but also as an issue with wider implications for family well-being and social and economic development. The ways in which families use and experience digital technologies can influence children's development, learning and skills, family relationships, access to opportunities, and participation in social and economic life. The report points toward digital environments in which families can benefit meaningfully from technological opportunities while responsibility for foreseeable risks is appropriately shared among families, public institutions, technology providers and other relevant actors. Family-centered and value-based approaches can help guide these choices while allowing Member Countries to adapt policies to their own institutional, legal, social and cultural contexts. In this way, the report seeks to translate enduring values into practical approaches that support families in a changing digital world.

INTRODUCTION

Family life has always been shaped by the social, cultural, and economic environments in which it develops. At the same time, families play an important role in shaping these environments by transmitting values, sustaining relationships across generations, nurturing children, providing care, and contributing to the social fabric of communities. These roles have wider implications for social and economic development, as family life influences the development of human capabilities, social well-being, and participation in economic and social life. Together, these contributions position the family as a backbone of development, connecting individual and family well-being with the wider development of society. In the OIC Member Countries, the family holds a particularly important place in social and cultural life, reflecting the strong influence of religious values, cultural traditions, and intergenerational ties.

Digital transformation has become an increasingly important part of this changing environment. The growing presence of digital technologies in everyday life has contributed to changes in patterns of communication, socialization, and intergenerational relations. The widespread use of social media platforms, online entertainment, digital consumer culture, virtual communities, and artificial intelligence-supported communication systems is reshaping aspects of family interaction, with implications for values, relationships, and social norms. Digital technologies also increasingly shape how family members learn, work, develop skills, access information and services, and participate in social and economic life. While digitalization offers significant opportunities for education, connectivity, and children's well-being, it also brings a range of risks and challenges for families and children.

Contemporary digital environments can present challenges related to excessive screen use, misinformation, online addiction, cyberbullying, exposure to inappropriate content, and reduced face-to-face family interactions. Internet addiction among young people may disrupt communication with parents and may influence attitudes and patterns of value transmission through exposure to diverse forms of digital content (SESRIC, 2017). In addition, technology or internet addiction associated with new technologies is recognized as a physical and psychological health concern (SESRIC, 2023).

For the OIC Member Countries, the interaction between technological developments and different social, cultural, and institutional contexts raises important governance questions. Global digital content flows may also interact in complex ways with local norms concerning privacy, authority, and moral responsibility.

The diversity of family structures and levels of digital access across the OIC Member Countries further underscores the importance of context-sensitive approaches. Average family size in OIC Member Countries ranges from 3.3 to 8.7 persons, with an overall average of 5.2, and family structures often include members from multiple generations, in line with historical and cultural traditions. At the same time, levels of digital access vary considerably. In OIC Member Countries, 63.6% of households have internet access, there are 107 mobile phones per 100 people, and computer ownership rates vary widely, from 99.51% to 2%. In 20 OIC Member Countries, household computer ownership exceeds 50% (SESRIC, 2023; 2024). These differences point to the importance of approaches that reflect different levels of digital access and capacity while addressing the implications of digital transformation for family life.

These developments point to the need to examine how digital transformation affects family life in the OIC Member Countries and how value-based and family-centered approaches can help address emerging challenges while enabling families to benefit from technological progress. This is important not only for family well-being, but also for wider social and economic development. The ways families use and experience digital technologies can influence children’s development, learning and skills, access to opportunities and services, and participation in social and economic life.

Prepared for the Standing Committee for Economic and Commercial Cooperation of the Organization of Islamic Cooperation (COMCEC), this report examines the nature and scope of digital threats to the family institution in the OIC Member Countries and explores value-based responses grounded in Islamic principles and cultural traditions. The report does not treat digital threats merely as an issue limited to children's online safety or individual screen use. Rather, the family institution is considered within a broader context encompassing communication, care, education, health, economic decision-making, privacy, and value transmission.

Accordingly, the analysis considers not only the effects of digital technologies on individual users but also their implications for family relationships, intergenerational ties, digital-platform practices, and public governance.

More specifically, the report examines how digitalization is shaping family life in Islamic Countries, including family relationships and well-being, the safety and development of children and young people, parenting practices, and transmission of values across generations. It considers both the opportunities and risks involved and explores how value-based digital family governance can respond to them. Rather than comparing or ranking countries according to their overall level of digitalization, the analysis focuses on how digital policies and practices affect families, the governance challenges that arise, and the policy responses that may be relevant.

The conceptual discussion provides a common framework for examining the global and OIC-level trends, regulatory frameworks, institutional arrangements, implementation mechanisms, and country cases that follow. The value framework serves as a structured basis for analysis rather than as a set of labels attached to individual initiatives. In this way, family relationships and well-being, children's development and safety, privacy and dignity, information integrity and shared responsibility guide the analysis throughout the report.

Methodologically, the report combines a synthesis of conceptual literature, a comparative review of international and national policy documents, contextual interpretation of selected indicators, and country case studies. The conceptual and value-based framework developed in the first section provides a consistent reference point for the analysis that follows.

The report is structured into five main sections, moving from conceptual framework to policy recommendations.

The first section establishes the conceptual and analytical framework of the report. It examines the role of the family as a social and civilizational institution, its contribution to social and economic development, and its foundations in Islamic thought. It also introduces the value framework used throughout the report, including the six core normative values and the cross-cutting guiding principles of Hikmah and Mas'uliyyah.

The second section examines the opportunities and risks associated with the digitalization of family life, with particular attention to family relationships and intergenerational ties, children's development and well-being, privacy, information integrity, and responsible digital participation.

The third section reviews emerging trends in family and digital governance at the global level and across OIC Member Countries, including regulatory and institutional approaches, coordination mechanisms, preventive measures, reporting and remedy, and emerging governance approaches and gaps.

The fourth section presents case studies of Türkiye, Malaysia, Jordan, Nigeria, and Hungary, examining regulatory frameworks, institutional arrangements, implementation mechanisms, and lessons that may be relevant to the OIC Member Countries.

Finally, the fifth section draws on the conceptual framework, comparative analysis, and country experiences to present policy recommendations for the OIC Member Countries, translating the report's family-centered and value-based perspective into practical policy priorities and an indicative implementation roadmap.

From a broader development perspective, the role of the family extends beyond the well-being of its individual members, contributing to human development and participation in social and economic life (SESRIC, 2023). In this context, supporting families in making safe and meaningful use of digital technologies can also strengthen their contribution to wider social and economic development.

1. CONCEPTUAL AND ANALYTICAL FRAMEWORK: FAMILY INSTITUTION AND ITS ISLAMIC VALUE FOUNDATIONS

1.1. Family as a Social and Civilizational Institution

The family is widely recognized as the most fundamental social institution and the foundation of human society. Across cultures and civilizations, it provides the primary environment in which individuals are born, nurtured, and socialized. Within the conceptual framework adopted in this report, and consistent with the Organization of Islamic Cooperation (OIC), the family is understood as a social institution established through the marriage of a man and a woman. As the building block of civilization, it serves as the primary setting for raising children, transmitting values, and ensuring the continuity of society while promoting stability, security, and human well-being (OIC, 2020, p. 6).

From a social science perspective, the family is one of the earliest and most influential environments for human development and a primary unit of social organization. It is within the family that children first develop cognitive, emotional, and social capacities through continuous interaction with parents and other caregivers, while also acquiring the values, norms, and responsibilities necessary for participation in society (Bronfenbrenner, 1979, pp. 3–42). Research on family socialization further highlights the central role of parents and caregivers in children's acquisition of values, social norms, and patterns of behavior that shape their participation in society (Grusec, 2011). Through relationships built on trust, reciprocity, and shared responsibility, families generate social capital that supports children's development, educational achievement, and social integration (Coleman, 1988, pp. S100–S108).

Beyond its role in individual development, the family performs essential functions that contribute to the well-being and stability of society as a whole. Strong family relationships can strengthen social well-being, reinforce intergenerational solidarity, preserve cultural identity, and transmit shared values across generations. Despite profound demographic, economic, and technological transformations, the family continues to play an important role in supporting individual well-being, intergenerational relationships, and the continuity of societies (SESRIC, 2023, pp. 5–7).

1.2. Family as the Backbone of Development

The role of families extends beyond individual and household well-being, contributing to broader social and economic development. Families contribute to long-term development by nurturing children, developing their capabilities, providing care across generations, and supporting strong relationships and participation in society. It is in this broader sense that the family can be understood as a backbone of development. At the same time, families are themselves shaped by wider economic and social conditions. The relationship between family well-being and development is therefore inherently two-way (SESRIC, 2023, pp. 5–7).

From a social development perspective, families play a central role in shaping individual well-being, social relationships, and the transmission of values across generations. The family provides an important setting for children's social and emotional development and for acquiring the knowledge, attitudes, and behaviors that influence their participation in society. It also provides care and mutual support at different stages of life, including for children, older persons, and persons with disabilities (SESRIC, 2023, p. 5). More broadly, childhood experiences can have lasting implications for educational attainment, health, social relationships, and other dimensions of well-being later in life (OECD, 2021d). Through these interconnected roles, families contribute to human development, intergenerational solidarity, and social well-being.

Families are also closely linked to economic development, particularly through their contribution to human capital formation. The conditions in which children grow up influence the development of their knowledge, skills, health, and social capabilities, with implications for learning, future employment, and participation in economic life. The family environment is particularly important during the early years, when the foundations for later learning and development are established (Naudeau et al., 2011). Families play a central role in creating the conditions that support children's healthy development, including care, safety, health and nutrition, and opportunities for learning. Supportive public services can strengthen families in fulfilling this role (World Health Organization et al., 2018). This connection between family life, human capital, and longer-term economic development is also evident in the OIC context. The family environment can shape children's educational attainment and academic achievement, as well as the skills, behaviors, and capacities that influence their future participation in economic life.

By supporting children's development from an early age, families therefore contribute not only to individual well-being but also to the formation of human capital that underpins longer-term economic development (SESRIC, 2017, pp. 12–13).

Care is another important way in which family life and economic participation are connected. The care provided within families to children, older persons, and those requiring support enables family members to participate in education, employment, and wider social life, although much of this contribution remains unpaid (Addati et al., 2018). The relationship between families and economic development also works in the other direction. Employment opportunities, income security, education, social protection, and access to essential services shape family well-being and families' capacity to provide care and support. Therefore, family well-being and socio-economic development should be understood as mutually reinforcing rather than as separate policy domains.

Digital transformation adds a new dimension to this relationship. Digital technologies can expand access to information, education, and services, facilitate communication and social connection, and help children and young people develop skills relevant to an increasingly digital society. However, the benefits of digitalization do not depend on access to technology alone. Families also need the skills, connectivity, institutional support, and other conditions required to use digital technologies effectively. The World Bank (2016) emphasizes that the potential of digital technologies to expand opportunities and improve service delivery depends on complementary factors, including skills and effective institutions. At the same time, digital environments can expose children and families to new or evolving risks, including harmful content and experiences, privacy concerns, online abuse, and other challenges affecting well-being. Current evidence therefore cautions against viewing digital technology as inherently beneficial or harmful, as its effects depend considerably on access, patterns of use, content, and the nature of online experiences (OECD, 2025; UNICEF, 2025). Unequal access to connectivity, suitable devices, digital skills, and appropriate support can also reinforce existing socio-economic inequalities (UNICEF Innocenti, 2025).

These developments have implications that extend beyond the digital environment itself. From a family-centered perspective, enabling families to benefit from digital technologies and protecting them from digital risks should therefore go hand in hand. Changes in family relationships, parental roles, children's development, patterns of interaction, and the transmission of values can affect families' ability to perform their wider social and developmental roles. At the same time, enabling families to use digital technologies effectively and in a balanced way can support learning, skills development, access to opportunities, and family well-being. This broader perspective is consistent with the OIC approach to family empowerment, which brings together areas such as education and employment, science and technology, economic development, child welfare, and family protection within a broader framework for strengthening families and their contribution to sustainable development (SESRIC, 2023, p. 7).

In this context, strengthening and supporting families in the digital age is relevant not only to family well-being but also to the broader social and economic development agenda. Family-centered and value-based approaches can help families benefit from the opportunities created by digital transformation while managing its risks and safeguarding the relationships, responsibilities, and values that sustain family life. In this way, strengthening the family institution in a changing digital environment can contribute to human development, social well-being, and sustainable social and economic development.

The role of the family in development also needs to be understood within the cultural, religious, and normative contexts in which family life takes place. In Islamic civilization, the family is understood not only in terms of its social and developmental roles, but also through a moral and value-based framework that defines responsibilities within the family and its relationship with the wider society.

1.3. Family in Islamic Civilization

The Qur'an presents the family as a divinely ordained institution and the natural foundation of human society. It emphasizes that humanity was created from a single soul and that men and women were created as complementary partners through whom future generations are established (Qur'an 4:1, An-Nisa). Accordingly, the family is understood not only as the natural environment for raising children but also as the primary setting for cultivating faith, character, compassion, and social responsibility.

Marriage, which forms the basis of the family, is regarded not merely as a private or contractual relationship but as a firm covenant (*mithaqan ghalizan*) that establishes the moral and legal foundation of family life (Qur'an 4:21, Surah An-Nisa). Islamic scholars interpret this expression as emphasizing that marriage creates a relationship of enduring commitment, mutual rights, and shared responsibilities rather than a simple legal agreement (Kamali, 2019; Al-Zuhayli, 2003).

Within this framework, the Qur'an describes the family as a source of tranquility (*sakinah*), love (*mawaddah*), and mercy (*raḥmah*):

> *"And of His signs is that He created for you from yourselves mates that you may find tranquility in them; and He placed between you affection and mercy. Indeed, in that are signs for a people who give thought." (Quran 30:21, Surah Ar-Rum)*

This verse highlights the emotional, ethical, and spiritual dimensions of the family as a space of mutual care, compassion, and stability. The Qur'an further portrays the ideal Muslim family as one in which spouses and children become "the joy of our eyes," while parents aspire to raise generations who serve as examples of righteousness:

> *"Our Lord! Bless us with spouses and offspring who will be the joy of our hearts, and make us models for the righteous." (Quran, 25:74, Surah Al-Furqan).*

Together, these verses present the family as a divinely ordained institution founded on compassion, mutual responsibility, and moral purpose. They portray the family not only as a source of emotional support and social stability but also as the primary environment in which faith, values, and righteous character are cultivated across generations.

Islamic scholarship further explains the significance of the family through the framework of the Maqasid al-Sharia (higher objectives of Islamic law). In particular, the family contributes directly to the protection of progeny (hifz al-nasl), while also supporting the preservation of faith (hifz al-din), intellect (hifz al-'aql), and human dignity (hifz al-'ird). From this perspective, the family is not only the means through which future generations are sustained but also the institution through which the broader objectives of Islamic law are realized and transmitted within society (Auda, 2008; Kamali, 2013).

In Islam, protecting and strengthening the family is therefore regarded not only as a social objective but also as a religious responsibility. This responsibility is rooted in the concept of *amanah* (trust), one of the fundamental ethical principles in Islam. The Qur'an describes *amanah* as a trust entrusted to humankind (Qur'an 33:72, Surah Al-Azhab), while family relationships are understood as one of its most significant manifestations. Accordingly, spouses, parents, and children are entrusted to one another by Allah and are expected to fulfil their mutual rights and responsibilities with justice, compassion, and accountability. This responsibility is further reinforced by the Qur'anic command:

> *"O you who have believed, protect yourselves and your families from a Fire whose fuel is people and stones." (Quran, 66:6, Surah At-Tahrim)*

Islamic scholars interpret this verse as placing a responsibility on parents and guardians to protect the moral, spiritual, intellectual, and physical well-being of their families through proper education, guidance, and ethical upbringing (Ibn Kathir, 2000; Al-Zuhayli, 2003). Accordingly, family protection extends beyond safeguarding family members from physical harm to nurturing faith, character, and values. A well-known hadith further reinforces this shared responsibility. The Prophet Muhammad (peace be upon him, PBUH) said:

> *"Each of you is a shepherd, and each of you is responsible for those under his care."*

He explained that a man is responsible for his household and a woman is responsible for her household and children, highlighting that every family member bear accountability according to his or her role (Sahih al-Bukhari, Hadith No. 7138; Sahih Muslim, Hadith No. 1829). Together, these teachings present family protection as a shared moral responsibility. In the Islamic worldview, safeguarding the family is therefore not merely a private matter but a collective trust that contributes to the preservation of faith, values, social solidarity, and the well-being of future generations.

Reflecting this perspective, Islamic scholars have regarded the family as the core institution upon which the health of society depends. Osman Bakar (2010, p. 9) compares the relationship between the family and society to that between a living cell and the human body: *just as healthy cells sustain the body, healthy families sustain civilization.* Protecting and strengthening the family is therefore viewed not only as a private concern but also as a collective responsibility contributing to social stability, moral continuity, and sustainable development.

One of the principal ways in which the family performs this broader social role is through the transmission of values from one generation to the next. Long before children enter formal education or engage with wider social institutions, they acquire fundamental beliefs, behaviors, and social norms within the family environment. Through daily interaction with parents and other family members, children learn responsibility, respect, empathy, honesty, and cooperation, laying the foundation for their personal development and social participation (Bronfenbrenner, 1979; Coleman, 1988).

In the Islamic worldview, value transmission is one of the family's central responsibilities. Parents are entrusted with nurturing not only the physical well-being of their children but also their moral and spiritual development. The Qur'an repeatedly emphasizes parental responsibility in raising righteous generations (Qur'an 66:6; 25:74), while the concept of *amanah* frames parenting as a trust that requires guidance, care, and accountability. Within family life, values are transmitted not only through explicit guidance but also through everyday relationships, parental example, and shared practices.

The transmission of values within the family extends beyond individual development and can also contribute to social solidarity and continuity across generations. Families that cultivate trust, mutual respect, solidarity, and ethical responsibility help build stronger communities and more resilient societies. As emphasized in the OIC Strategy for the Empowerment of the Marriage and Family Institution, strengthening families is closely linked to preserving social stability, reinforcing shared values, and promoting sustainable development (OIC, 2020).

In an era of rapid digital transformation, the family's role as the primary institution for value transmission has become even more critical. While digital technologies provide unprecedented opportunities for learning, communication, and participation, they also reshape how children acquire information, form identities, and interact with others. This changing environment increases the importance of families in helping children develop ethical judgement, digital responsibility, and resilience. Consequently, strengthening families is not only a social objective but also a strategic investment in building value-based and digitally resilient societies.

1.4. Understanding Digital Family Governance

Understanding the role of families in an increasingly digital world requires looking beyond the home itself. Family life is influenced not only by relationships within the household but also by public policies, schools, technology companies, legal and regulatory frameworks, and wider social and cultural developments. Looking at these different influences naturally leads to a broader discussion about governance.

The concept of governance has evolved over time. Rather than referring only to the exercise of state authority, it is now commonly understood as the ways in which governments, private actors, and civil society work together to address shared challenges and pursue common goals. In this sense, governance extends beyond government action and includes collaboration, interaction, and shared responsibility across different sectors (Bevir, 2012, pp. 19–21, 28, 42).

This broader understanding is also reflected in discussions on digital transformation. As digital technologies have become part of everyday life, digital governance has come to include not only technical regulation but also ethical issues, institutional coordination, digital rights, responsible innovation, and public trust. International frameworks similarly emphasize values such as human dignity, human rights, transparency, accountability, inclusion, and social well-being, while highlighting the importance of cooperation among different stakeholders (UNESCO, 2021, paras. 10–17).

Within this context, families are often seen mainly as beneficiaries of digital policies or as environments where children need protection. However, growing research suggests that children's digital experiences are shaped not only by technological safeguards but also by everyday family practices, parental guidance, shared learning, and open communication at home (Livingstone & Blum-Ross, 2020, pp. 18–31, 64–78). This points to a broader role for families in shaping children's digital experiences.

Against this background, the concept of "digital family governance" is used in this report to highlight the role of families within the wider digital ecosystem. It recognizes that families do not act alone. Governments, educational institutions, technology companies, civil society organizations, faith communities, and families each have a role in creating digital environments that support children's development and family well-being.

For the purposes of this report, *digital family governance* refers to the ethical, institutional, and relational processes through which families and other societal actors influence the development, use, and governance of digital technologies in ways that support children's well-being, strengthen families, and contribute to the common good. The following section builds on this understanding by outlining an Islamic value-based framework for digital family governance.

1.5. Viewing Digital Family Governance Through Core Islamic Principles

Recent scholarship challenges the assumption that digital technologies and cybersecurity are value-neutral or purely technical domains. Instead, their design, governance, and use inevitably involve moral choices, ethical responsibility, and principled governance (Auladi & Muwahid, 2025). Accordingly, scientific and technological development cannot be separated from ethical reflection. Technological progress should be guided by ethical values and a clear sense of purpose rather than by technical considerations alone (Bakar, 2018). Viewed in this way, digital family governance is not merely a technical or regulatory exercise but an ethical undertaking requiring sound judgment, accountability, and value-based stewardship to ensure that digital environments contribute positively to child development and family well-being. (Auladi & Muwahid, 2025).

More importantly, this value-based approach reflects a broader civilizational perspective. Every civilization is shaped by a particular worldview and conception of reality that informs its institutions, norms, and social order (Kalın, 2010, p.1). From this perspective, digital family governance cannot be understood solely as a technical or regulatory issue; it also reflects deeper assumptions about the purpose of technology, human well-being, and the role of the family in society.

Within this broader framework, Islamic ethical values provide a normative foundation for responsible decision-making and value-based governance in the digital age (Auladi & Muwahid, 2025). Rather than functioning as isolated concepts, these principles can be understood as part of a broader ethical framework relevant to family life, social relations, public policy, and societal well-being. In the context of digital transformation, they provide a basis for considering how technological development can support child development, family well-being, responsible digital behavior, and the common good.

In the digital age, this value-based approach is essential for achieving the Qur'anic aspiration of raising children who become "the joy of our hearts" (Qur'an 25:74), which requires guiding them in both their physical-emotional growth and their ethical engagement with digital tools.

While this report maintains a dedicated focus on digital family governance, this approach is aligned with broader emerging frameworks such as "Islamic Digital Civilization" (Hussin, 2025; Ali et al., 2025) and "Islamic Technology" (Kadir, 2025). These civilizational perspectives reflect a growing scholarly movement that frames digital transformation through Islamic ethics, emphasizing that technological development must serve human well-being rather than existing as an end in itself (Hussin, 2025).

The value-based conceptual framework presented in this report is organized around two complementary components. The core normative values are Amanah (trust and stewardship); Hifz (protection of the family, progeny, and intellect); Adab and Haya (ethical conduct, dignity, modesty, and privacy); Sidq (truthfulness and information integrity); Amr bil-Ma'ruf wa Nahy'an al-Munkar (promoting good and preventing wrongdoing); and Wasatiyyah (balance and moderation). Two cross-cutting guiding principles, Hikmah (wisdom) and Mas'uliyyah (responsibility), provide the interpretive and implementation lens through which these values are contextualized and translated into responsibilities for relevant actors. This framework provides a common reference for considering the implications of digital transformation for families throughout the report.

1.5.1. Core Normative Values

1.5.1.1. Amanah (Trust and Stewardship)

Amanah (trust) is a foundational ethical principle in Islam, referring to what is entrusted to one's care and the responsibility to act faithfully in relation to that trust (TDV Encyclopedia of Islam, "Emanet"). Rooted in the Qur'anic concept of trust (Qur'an 33:72) and reinforced by the Islamic understanding of responsibility toward those under one's care (Qur'an 66:6; Sahih al-Bukhari, Hadith No. 7138; Sahih Muslim, Hadith No. 1829), amanah emphasizes care, integrity, and accountability in fulfilling one's responsibilities toward others (Kamali, 2019; Altalib et al., 2024). It also extends beyond the fulfillment of formal duties to the cultivation of trustworthiness in personal and social relationships (Kasim et al., 2020).

In the context of digital governance, amanah provides an ethical basis for considering responsible stewardship, particularly in relation to data, privacy, safety, and the exercise of institutional and technological power. Recent scholarship has explored amanah and related concepts of trusteeship as a basis for considering ethical responsibility in relation to digital technologies and artificial intelligence. From this perspective, responsible digital governance extends beyond technical compliance to questions of accountability, trust, and the responsible exercise of technological power. (Ali et al., 2025; Serevan, 2025)

Within the value framework developed in this report, amanah is reflected in digital family governance at two levels:

- **Parental Guidance & Empowerment**: Emphasizes parents' responsibility to guide and support children's digital engagement, including through digital literacy, critical thinking, ethical online behavior, balanced technology use, and protection from online risks.
- **Institutional & Shared Accountability:** Recognizes that protecting children in digital environments is not the responsibility of parents alone. Schools, public institutions, technology companies, and digital service providers also have responsibilities in creating safer and more trustworthy digital environments.

Digital Family Governance Insight

Through the principle of **amanah**, digital family governance emphasizes responsible stewardship, accountability, and shared responsibility for protecting and supporting children in digital environments.

1.5.1.2. Hifz (Protection of the Family, Progeny and Intellect)

The protection of the family (hifz al-usra), progeny (hifz al-nasl), and intellect (hifz al-'aql) represent complementary dimensions of Hifz that together support human well-being across generations. While hifz al-nasl and hifz al-'aql are traditionally recognized among the higher objectives of Islamic law (Maqasid al-Shariah), hifz al-usra has received increasing attention in contemporary Islamic scholarship and OIC policy frameworks, reflecting the importance of protecting and strengthening family life and social well-being (Kamali, 2019; Auda, 2008; OIC, 2020).

In the context of digital transformation, these dimensions of Hifz provide a basis for considering different aspects of family and child protection in digital environments. Contemporary research also highlights the importance of parental guidance, children's rights and well-being, digital literacy, and critical engagement with digital technologies (Livingstone & Blum-Ross, 2020; OECD, 2025; UNICEF Innocenti, 2025). Within the Hifz framework developed in this report, these concerns are reflected in the following three areas:

- **Protecting the Family (*Hifz al-Usra*):** In the digital context, this includes strengthening parents' capacity to guide and support children in their use of digital technologies.
- **Protecting Progeny (*Hifz al-Nasl*):** In the digital context, this includes protecting children's rights and dignity and supporting their healthy moral, emotional, and social development.

- **Protecting Intellect (*Hifz al-'Aql*):** In the digital context, this includes strengthening digital literacy and critical thinking and protecting children's learning, development, and well-being from harmful digital experiences.

Digital Family Governance Insight

Through **Hifz (protection of the family, progeny, and intellect)**, digital family governance seeks to safeguard children from digital risks while supporting family well-being and children's intellectual, moral, emotional, and social development.

1.5.1.3. Adab and Haya (Ethics, Modesty and Privacy)

Adab (proper conduct) and *haya* (modesty and moral restraint) are closely interconnected values that shape personal conduct and social interaction in Islam. While adab emphasizes respect, kindness, honesty, and proper conduct in relationships, haya emphasizes modesty, dignity, self-restraint, and respect for personal boundaries (TDV Encyclopedia of Islam, "Edep"; "Hayâ"). Together, these values provide an ethical basis for protecting individual dignity and privacy (Qur'an 24:27–31; 49:11–12).

Contemporary discussions of Islamic digital ethics have emphasized the relevance of Islamic values to conduct and interaction in digital environments (Hussin, 2025; Iqbal & Kanus, 2026). Research addressing privacy from an Islamic ethical perspective also highlights the importance of protecting personal information and respecting privacy in digital environments (Alwi et al., 2014). Within the value framework developed in this report, adab and haya provide guidance for considering respectful conduct, dignity, privacy, and personal boundaries in digital family governance.

These considerations are reflected in three areas:

- **Respectful Communication & Digital Citizenship:** Encourages constructive and respectful online communication, responsible content creation, and empathy, while providing an ethical basis for addressing cyberbullying, online harassment, hate speech, and other forms of harmful digital interaction.
- **Privacy & Data Stewardship:** Supports the protection of personal data, sensitive family information, and personal boundaries, while discouraging intrusive practices and the unauthorized sharing of private content.
- **Protection of Dignity:** Emphasizes the importance of children and family members interacting in digital environments in ways that uphold their own dignity and respect the dignity and personal boundaries of others.

Digital Family Governance Insight

Through **adab** and **haya**, digital family governance promotes respectful conduct, privacy, dignity, and responsible behavior in digital environments.

1.5.1.4. Sidq (Truthfulness and Integrity)

Sidq (truthfulness) is a core Islamic value that emphasizes honesty, sincerity, and integrity in intention, word, and action (TDV Encyclopedia of Islam, "Sıdk"). The Qur'an explicitly commands believers to uphold truthfulness and integrity in their dealings (Qur'an 9:119; 33:70), while the Prophet Muhammad (PBUH) described truthfulness as a defining characteristic of righteousness (Sahih Muslim, Hadith No. 2607).

In the digital realm, sidq provides a normative basis for promoting information integrity and responsible communication. Contemporary scholarship on Islamic digital ethics has linked truthfulness and related ethical principles to challenges such as misinformation, deception, and manipulation in digital environments (Hussin, 2025; Abd Kadir et al., 2026). Addressing misinformation therefore has not only technical and regulatory but also ethical dimensions in maintaining trustworthy digital environments.

Within the value framework developed in this report, these concerns are reflected at two levels:

- **Empowering Families & Children:** Highlights the importance of developing critical thinking and media literacy skills in children, enabling them to evaluate online content critically, verify information before sharing, and resist digital manipulation.
- **Platform Accountability & Governance:** Emphasizes transparency, authenticity, and accountability among digital content providers and platforms, supporting more reliable and trustworthy information ecosystems.

Digital Family Governance Insight

Through **sidq**, digital family governance supports truthful communication, information integrity, and the development of critical media literacy.

1.5.1.5. Amr bil-Ma'ruf wa Nahy'an al-Munkar (Promoting Good and Preventing Wrongdoing)

Amr bil-Ma'ruf wa Nahy 'an al-Munkar (promoting what is right and preventing wrongdoing) is a foundational Islamic principle concerned with promoting what is good and preventing what is wrong (TDV Encyclopedia of Islam, "Emir bi'l-Ma'rûf Nehiy ani'l-Münker"). The Qur'an presents this principle in relation to both individual and collective responsibility for encouraging what is right and discouraging wrongdoing (Qur'an 3:104; 3:110; 9:71).

Within the value framework developed in this report, this principle is reflected in digital family governance through two complementary areas:

- **Preventing Online Harms (*Nahy 'an al-Munkar*):** Emphasizes efforts by families, public institutions, technology companies, and other relevant actors to reduce children's exposure to harmful, deceptive, or inappropriate content, online abuse, and other digital risks.
- **Promoting Beneficial Digital Spaces (*Amr bil Ma'ruf*):** Emphasizes digital environments that provide children and families with access to beneficial, educational, and age-appropriate content and opportunities. For families, this includes guiding children toward constructive digital participation and media literacy rather than relying solely on restrictions. Technology providers and other relevant actors can also contribute by expanding the availability of safe, child-friendly, and beneficial digital resources.

Digital Family Governance Insight

Through **Amr bil-Ma'ruf wa Nahy 'an al-Munkar**, digital family governance encourages beneficial and responsible digital participation while seeking to prevent harmful online content and practices.

1.5.1.6. Wasatiyyah (Balance and Moderation)

Wasatiyyah (balance and moderation) is an Islamic principle that emphasizes balance and avoidance of excess. The Qur'an characterizes the Muslim community as a "middle community" (ummatan wasatan) (Qur'an 2:143), a concept associated with moderation, balance, and justice in Islamic thought (TDV Encyclopedia of Islam, "Vasat").

In the digital context, wasatiyyah provides a basis for considering how technological opportunities can be used without losing sight of the risks associated with excessive or harmful forms of digital engagement. Contemporary discussions of Islamic digital ethics have similarly drawn attention to moderation and balanced engagement in the use of digital technologies (Hussin, 2025). From this perspective, the emphasis is neither on rejecting digital technologies nor on accepting their use without sufficient attention to their effects on individuals and families.

Research on children's digital lives similarly points to the importance of considering both the opportunities associated with digital technologies and potential risks to children's well-being, rather than treating digital engagement as inherently beneficial or harmful (OECD, 2025; UNICEF Innocenti, 2025).

Within the value framework developed in this report, these considerations are reflected through wasatiyyah across three areas:

- **Balanced Digital Use:** Encourages healthy boundaries around screen use, gaming, social media, and other digital activities, with attention to family relationships and children's well-being.
- **Purposeful Use of Digital Technologies:** Encourages families and children to make meaningful use of digital tools for learning, skills development, creativity, communication, and other beneficial purposes.
- **Digital Well-being:** Draws attention to the need to balance the opportunities offered by digital technologies with their possible effects on physical, mental, and relational well-being.

Digital Family Governance Insight

Through **wasatiyyah**, digital family governance encourages balanced and purposeful engagement with technology while supporting family well-being and children's healthy development.

While the preceding sections introduce the core normative values of the framework, applying these values in complex digital environments also requires guidance on how they should be understood and translated into action. Rather than introducing additional values, *hikmah and mas'uliyyah* serve as two complementary guiding principles, supporting sound judgement and responsible action in policy, institutional, and family contexts.

1.5.2. Cross-Cutting Guiding Principles

1.5.2.1. Hikmah (Wisdom)

In Islamic thought, hikmah (wisdom) is more than knowledge. It involves using knowledge with sound judgment, understanding the context of a situation, and making decisions with attention to their purpose and consequences. Rather than treating knowledge as an end in itself, hikmah is concerned with its wise and responsible application (Qur'an 2:269; al-Raghib al-Iṣfahani, as cited in TDV Encyclopedia of Islam, "Hikmet"). Classical Islamic scholars have also associated hikmah with sound judgment in thought and action and with placing things in their proper context (al-Ṭabari and Ibn al-Arabi, as cited in TDV Encyclopedia of Islam, "Hikmet"). This understanding is consistent with the maqasid approach, which emphasizes higher ethical purposes and consideration of the wider consequences of decisions (Auda, 2008).

Applied to digital family governance, hikmah begins with a simple observation: technologies are not merely neutral tools; their design and use can shape human choices, relationships, and social practices (Winner, 1980, pp. 121–125). This is particularly relevant in contemporary digital environments, where platforms, algorithms, and digital devices increasingly influence how people communicate, access information, and make decisions. From this perspective, hikmah encourages families, educators, technology developers, and policymakers to look beyond novelty, convenience, or technical efficiency and consider a more fundamental question: What purpose do these technologies serve? Their value can therefore be considered in terms of their contribution to human well-being, strong families, and the common good, rather than novelty or commercial success alone.

Hikmah also draws attention to both the immediate and longer-term consequences of digital choices. Different circumstances may call for different responses, considering children's developmental stages, family circumstances, cultural settings, and the nature of the technology involved (Auda, 2008). Research on children's digital lives similarly highlights the importance of considering both the opportunities offered by digital technologies and their possible implications for privacy, family relationships, well-being, and children's future interests (Livingstone & Blum-Ross, 2020, pp. 64–78; Steinberg, 2017, pp. 851–855). Within the value framework developed in this report, these considerations are reflected through hikmah in balanced and context-sensitive judgment rather than one-size-fits-all responses.

Finally, hikmah supports critical engagement with digital content rather than passive consumption. Classical understandings of hikmah include soundness in word and action and the ability to distinguish truth from falsehood (Kutluer, 1998). In digital environments, this provides a basis for emphasizing critical digital literacy and moral judgment alongside technical safeguards. It encourages individuals to question information, recognize manipulation and misinformation, and consider how digital environments may influence attention, choices, and behavior. In this sense, hikmah supports conscious and critical engagement with digital technologies.

Digital Family Governance Insight

In practice, **hikmah** encourages decision-making that is purpose-oriented, context-sensitive, balanced, future-aware, and guided by critical discernment.

1.5.2.2. Mas'uliyyah (Responsibility)

In Islamic thought, mas'uliyyah (responsibility) refers to the moral responsibility that accompanies human agency and accountability. Individuals are responsible for their actions and choices, and this responsibility is closely connected to the duties and trusts they undertake (Qur'an 17:36; TDV Encyclopedia of Islam, "Sorumluluk"). Responsibility also extends beyond the individual, as people assume different responsibilities within families, communities, and institutions according to their roles and the authority entrusted to them.

Applied to digital family governance, mas'uliyyah draws attention to the responsibilities of different actors across the digital environment. Parents, educators, technology companies, governments, religious institutions, civil society organizations, and other relevant actors have different but complementary roles in protecting children and supporting families. This understanding is consistent with the Prophetic teaching, “Each of you is a shepherd, and each of you is responsible for those under your care” (Sahih al-Bukhari, no. 7138; Sahih Muslim, no. 1829). It also reflects the Qur'anic emphasis on accountability for one's actions and choices (Qur'an 17:36). From this perspective, protecting children and supporting families in digital environments cannot rest on parents alone but requires responsibility to be shared among the relevant actors.

Mas'uliyyah also draws attention to the accountability that accompanies authority. The Qur'anic concept of amanah (trust) emphasizes responsibility for what is entrusted to one's care (Qur'an 33:72), while the concept of khalifah (stewardship) is associated with human responsibility in the exercise of authority and stewardship (Qur'an 2:30).

In digital family governance, these principles provide a basis for considering the responsibilities associated with the design, development, regulation, and use of digital technologies, data, and artificial intelligence. Contemporary approaches to digital governance similarly emphasize transparency, accountability, human oversight, and responsibility in the development and use of artificial intelligence (OECD, 2019; UNESCO, 2021). Research and international guidance on children's digital lives also emphasize age-appropriate protection, digital literacy, and supportive environments for children and families (UNICEF, 2020).

Within the value framework developed in this report, mas'uliyyah therefore emphasizes shared but differentiated responsibility. Families, schools, public institutions, technology companies, faith communities, and civil society contribute in different ways to protecting children and supporting family well-being. This is also consistent with the Qur'anic call to "cooperate in righteousness and piety" (Qur'an 5:2).

Digital Family Governance Insight

In practice, **mas'uliyyah** encourages action that is responsible, accountable, collaborative, and focused on protecting children, strengthening families, and serving the common good.

Although closely interconnected, Hikmah and Mas'uliyyah perform distinct yet complementary functions within the proposed value-based framework. Hikmah guides ethical judgement by helping to consider what is appropriate in a given context, while Mas'uliyyah draws attention to responsibility, accountability, and the roles of different actors in translating ethical commitments into action. Their complementary roles are summarized in Table 1.1.

Table 1.1 Complementary Roles of Hikmah and Mas'uliyyah in Digital Family Governance

Hikmah (Ethical Judgement)	Mas'uliyyah (Ethical Responsibility)
What is the purpose?	Who is responsible?
What is appropriate in this context?	Who is accountable?
What is trustworthy and ethically sound?	Who needs protection, and who is responsible for providing it?
How can benefits and potential harms be balanced?"	Who has responsibility for the use of authority and resources?
What are the long-term consequences?	How can shared responsibility become collective action?

Source: Based on the conceptualization of Hikmah and Mas'uliyyah and the supporting sources discussed in this section (Auda, 2008; Kutluer, 1998; TDV Encyclopedia of Islam).

Together, Hikmah and Mas'uliyyah provide complementary guidance for applying the core normative values to digital family governance. Hikmah supports context-sensitive judgement and consideration of competing interests, while Mas'uliyyah draws attention to responsibility, accountability, and the roles of different actors in translating ethical commitments into action. Table 1.2 shows how these guiding principles relate to each of the core normative values.

Table 1.2 Applying Islamic Values through Hikmah and Mas'uliyyah

Core Normative Value	Hikmah – Guiding Judgement	Mas'uliyyah – Guiding Responsibility and Action
Amanah	Considers whether digital technologies are used in ways that reflect trust, responsible stewardship, human well-being, and the common good.	Draws attention to the responsibilities and accountability of parents, technology companies, governments, and other relevant actors in fulfilling that trust.
Hifz (Protection of the Family, Progeny and Intellect)	Considers how digital decisions affect family relationships and children's well-being, including their longer-term implications, and supports critical and balanced engagement with digital environments.	Draws attention to responsibilities for protecting children, supporting family well-being, and safeguarding children's intellectual, emotional, and social development through appropriate safeguards, education, regulation, and family-centered policies.
Adab and Haya	Guides judgement on appropriate digital conduct according to context and relationships, with attention to dignity, modesty, privacy, and respect for personal boundaries.	Draws attention to the responsibilities of individuals, families, educators, institutions, and technology providers in upholding respectful conduct, privacy, and dignity in digital environments.
Sidq	Guides judgement on the truthfulness, reliability, and integrity of digital information.	Emphasizes honesty, transparency, accountability, and responsible communication in digital environments.
Amr bil-Ma'ruf wa Nahy 'an al-Munkar	Supports judgement in distinguishing beneficial from harmful digital content, behaviors, and practices.	Draws attention to the roles of families, educators, technology companies, governments, and civil society in promoting beneficial digital environments and preventing harmful practices through education, policy, and collective action.
Wasatiyyah	Supports balanced judgement concerning the opportunities, competing interests, and potential harms associated with digital technologies.	Encourages responsible action that takes account of context, evidence, and the need for balance in digital governance.

Source: Based on the conceptualization of the core normative values, Hikmah, and Mas'uliyyah and the supporting sources discussed in this section.

This framework does not introduce new ethical concepts. Rather, it brings together established Islamic principles and considers their relevance to contemporary digital family governance. The following chapters draw on these principles where they help explain the impacts of digitalization on families and children, clarify responsibilities, identify what needs to be protected, and guide decisions on issues such as information, privacy, balance, and context. The aim is not to attach Islamic terminology to individual policies, but to use these principles where they provide meaningful guidance.

2. DIGITALIZATION AND THE CHANGING NATURE OF FAMILY

2.1. Conceptualizing the Digitalization of Family Life

Digitalization of family life refers to the growing integration of digital technologies, platforms, data systems, and algorithmic services into communication, care, education, consumption, entertainment, and access to public services. In this report, the concept is examined through the analytical framework established in Section 1.5. Accordingly, the key question is not whether technology is present in family life, but how particular digital arrangements affect family relationships, children's development and intellect, privacy and dignity, information quality, responsibility, and the balance between protection and meaningful participation.

Instant messaging applications, social media, and other digital communication technologies have become increasingly integrated into everyday family life. Family relationships and interactions therefore increasingly extend beyond the physical household, as digital technologies enable family members to remain connected across households and geographical distances (Taipale, 2019).Rather than replacing face-to-face communication through a one-way transformation, digital communication moves interaction among family members toward a "polymedia" environment in which different forms of communication are used together. Instant messaging, video calls, voice messages, and social media enable families to remain connected throughout the day, respond asynchronously, and sustain kinship ties across geographical distances. However, being constantly connected can increase expectations of availability and create the risk that emotional depth may diminish even as the frequency of communication rises (Madianou & Miller, 2012). Whether they are digital immigrants or digital natives, family members come together on digital platforms for purposes such as conversation, social media use, and shopping. This trend increasingly shapes relationships among family members and contributes to the emergence of what has been described as the digital family. (Taipale, 2019).

The "digital family" is defined not merely as a household that owns digital tools, but as a relational structure in which communication, care, decision-making, access to services, and value transmission among family members are carried out in continuous interaction with digital systems. Taipale (2019), for example, describes the "digital family" as a family whose members use information and communication technologies and social media applications at a basic level to maintain or strengthen their ties. Even when family members are geographically distant from one another, intergenerational communication can be sustained through digital tools. Platformization transforms family life from a collection of independent applications into an interconnected data ecosystem that brings together functions such as communication, entertainment, education, health monitoring, children's school records, and access to public services. This transformation can reduce time and space constraints for families. However, every technology entail risks as well as opportunities. Accordingly, the digital family faces multiple risks.

The misuse of digital technologies may cause family members to become mentally and emotionally distant from one another, even when they live under the same roof. This may lead to conflicts between different perspectives within the family, where fundamental values are acquired, communication deteriorates, mutual attention among family members declines, and family privacy is violated (Yürekli, 2022). The term "technoference" refers to interruptions in interpersonal interactions or shared time caused by digital technology use (McDaniel & Radesky, 2018)."Parental technoference" refers to regular interruptions to real-time, face-to-face communication, interaction, or shared time among family members resulting from parents' technology use (Komanchuk et al., 2023). Technoference within the family, in particular, may weaken the parent-child bond and may create problems in interaction, communication, and social relationships. Family members checking their phones at the dinner table or parents scrolling through social media videos while spending time with their children are examples of this phenomenon (McDaniel & Radesky, 2018). The literature indicates that technoference affects children's health and development (Komanchuk et al., 2023), reduces parental responsiveness, and may prevent children from receiving the emotional feedback they expect during communication. Research has also associated parental technoference with changes in parent-child interaction and children's behavioral and developmental outcomes (Komanchuk et al., 2023). Studies of younger children further suggest that technology-related interruptions during parent-child interaction may affect aspects of early language development (Konrad et al., 2021).

Another effect of digitalization is the reduction of interaction within the family. The concept of "alone together," introduced by Turkle (2011), explains one of the fundamental paradoxes of digital family life. Family members may be physically present in the same environment while directing their attention to different screens and becoming emotionally distant from one another. Nevertheless, this concept should not be interpreted as meaning that technology inevitably weakens family ties. What is decisive is whether devices interrupt shared family time, whether co-use supports interaction, and whether family members can develop common rules regarding digital boundaries.

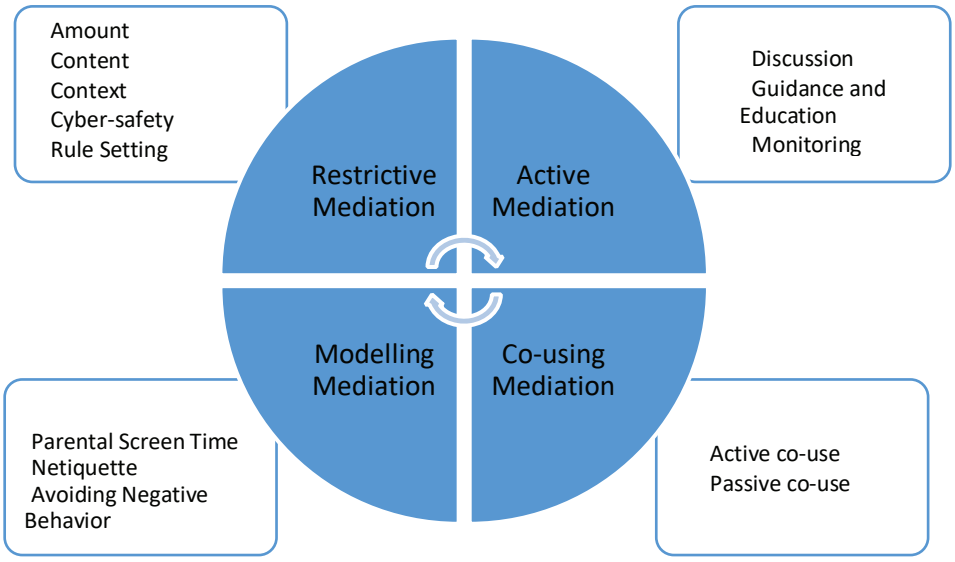
Digitalization also diversifies the environments in which socialization takes place. Traditional socialization processes centered on the family, school, neighborhood, and kinship networks are expanding to include online gaming communities, social media networks, and virtual interest groups. While these environments may offer children and young people opportunities for belonging, creativity, and peer support, they may also pose risks, including the performative construction of digital identity, exclusion, peer pressure, and online norms that take precedence over family values. The quality of online socialization should therefore be assessed not only by the duration of use but also by the safety, reciprocity, and developmental appropriateness of the relationships formed.

Inequality in digital access is expressed through the concept of the digital divide (Cullen, 2001). A range of family-related and societal factors shapes the digitalization of the family. The family's socio-economic status (SES) is a comprehensive indicator of these factors (Conger et al., 2010). Research shows that families with lower SES benefit less from digital opportunities than families with higher SES (Chang et al., 2016). Similarly, the digital divide may create inequalities arising from access to digital information and communication technologies. It may also make broader social inequalities between SES groups more visible (Shi et al., 2024). For example, families with lower SES tend to have fewer technological resources and more limited access to digital technologies than families with higher SES. As a result, children from higher-SES families may demonstrate greater self-efficacy and digital skills than their lower-SES peers. Hadasik and Krol (2024) identified various socio-demographic factors affecting the digital divide, including age, education level, household economy, cultural factors, and region. The comprehensive literature review by Srinuan and Bohlin (2011) similarly identified antecedents including infrastructure, socio-economic status, knowledge and skills, psychological factors, culture, service quality, and institutional and administrative factors.

Digitalization is also changing how knowledge and guidance are shared within families. Children may develop confidence and practical skills in using digital technologies from an early age, while parents continue to play an important role in guiding how these technologies are used at home (Soyoof et al., 2024). This role extends beyond managing screen use and includes helping children make safe and responsible choices, respond to online risks, protect their privacy, and develop the skills needed to use digital technologies meaningfully (Tan et al., 2024). As a result, digitalization does not simply shift knowledge or authority from one generation to another. Rather, it creates new areas in which children’s growing digital experience and parents’ continuing responsibility for guidance need to work together. The conditions described above highlight the growing importance of digital parenting. Digital parenting encompasses parents' provision of access to digital tools, their use of these tools together with their children, and their regulation and guidance of digital life while preserving the family's fundamental values. Digital parenting is defined as a contemporary and critical issue that enables family members to benefit effectively from digital technologies while being protected from the risks arising from their use (Livingstone & Blum-Ross, 2020). It is understood not merely as monitoring and restriction, but as a relational approach encompassing shared learning, open communication, age-appropriate autonomy, digital resilience, and collaborative problem-solving (Livingstone & Blum-Ross, 2020).

In this context, parental roles in digital families are addressed within the framework of parental mediation. This approach recognizes parents as role models and active regulators in their children's digital lives. Parents are expected to provide their children with digital access, monitor and regulate their children's digital behavior, safeguard the children's best interests, and mitigate digital risks when necessary. Figure 2.1 presents Fam et al.'s (2025) classification of parental mediation strategies across four dimensions. These mediation practices are also shaped by family involvement and the socio-cultural context in which children's digital activities take place (Soyoof et al., 2024).

Figure 2.1 Parental Mediation Strategies



Source: *Fam et al., 2025*

Restrictive Mediation: Parents limit their children's digital lives by establishing rules regarding how much, for what purposes, and in what contexts the internet may be used in order to support children's cyber safety.

Active Mediation: Parents proactively mediate the family's digital life by monitoring media consumption and patterns of use and by actively guiding their children's media use through education and discussion.

Co-using Mediation: Rather than providing explicit guidance and instructions, parents offer indirect behavioral cues and expect children to internalize good digital practices and continue to display these behaviors even when their parents are not present.

Modeling Mediation: Parents intentionally or unintentionally model good practices in digital life, such as online etiquette and moderate screen use.

When the effects of digitalization on the family are considered together, it becomes clear that its impact on family interaction and relationships cannot be explained solely by the presence or duration of technology use. The principal factors shaping outcomes are whether use is shared or individual, platform design, the family's socio-economic resources, parental self-efficacy, intergenerational communication, the safety of online relationships, and family members' ability to develop shared boundaries. Accordingly, the analysis of the risks and opportunities created by digital technologies examines their context-dependent effects rather than categorically describing technologies as either positive or negative.

2.2. Digital Opportunities for Family and Child Well-Being

Every technology generates risks and opportunities for society (Fischhoff et al., 1984). Assessing risks relative to opportunities constitutes a distinct field of inquiry in industrial and policy contexts. However, because risks and opportunities are closely interrelated, efforts to reduce risks may also prevent societies from benefiting from available opportunities (Fischhoff et al., 1978). Digital risks and opportunities are therefore widely debated among stakeholders, particularly in relation to children and families. Depending on the purpose of use, user characteristics, family resources, platform design, and parental mediation, a technology may produce both supportive and harmful outcomes. The assessment of digital technologies, therefore, concerns not simply their benefits or harms, but which benefits and which harms arise, for whom, and under what conditions.

The digital environment has become a fundamental part of everyday life, bringing significant changes to the ways children and families learn, communicate, and engage with the world around them.

According to the Organisation for Economic Co-operation and Development (OECD, 2025), digital technologies offer highly valuable opportunities for learning, entertainment, access to information, discovery of new concepts, and connection with peers.

One of the most visible opportunities created by digitalization lies in education. The spread of digital technologies has made educational resources more widely accessible, extending the boundaries of traditional education. This has been particularly beneficial in enabling learning to move beyond formal educational settings. Beyond individual learning, digital technologies also offer important opportunities to strengthen family dynamics and increase parents' involvement in their children's education. A report by the United Nations Educational, Scientific, and Cultural Organization (UNESCO) (Nicolai et al., 2023) emphasizes that educational technologies ranging from mobile messaging applications to comprehensive digital learning platforms have become increasingly important in narrowing the communication gap between school and home. These tools support more active and sustained parental involvement in children's learning processes, including among social groups with limited access to services.

Digital health applications also offer significant opportunities for family well-being. Technology-based practices such as telemedicine, remote monitoring, online psychological counseling, family counseling, and digital parenting support programs can reduce barriers of time and distance, particularly for families living in rural areas, in places where the number of specialists is limited, or where caregiving responsibilities make access to services difficult. However, the sustainability of these opportunities depends on the integrated design of connectivity quality, digital skills, service standards, data privacy, and referral mechanisms for face-to-face support (Bradford, Caffery, & Smith, 2016).

Patterns of digital use vary by age, platform, household resources, educational context, and the purpose for which technologies are used. These differences matter because the same amount of screen exposure can involve very different developmental and relational experiences. For digital family governance, the relevant policy question is therefore not simply how long children are online, but what they are doing, with whom, under what design conditions, and with what family support.

2.3. Digital Risks to Family Integrity, Socialization and Values

The rapid spread of digital technologies offers children unprecedented opportunities for access to education, information, creativity, and social participation, while also creating new risks. The OECD has mapped the risks children encounter in digital environments (Table 2.1). Under this framework, sources of risk are classified as content, conduct, contact, and consumer risks. In addition, the proliferation and interaction of advanced technologies have given rise to cross-cutting risks (OECD, 2021).

Table 2.1 Risks for Children in the Digital Environment

Risk Categories	Content Risks	Conduct Risks	Contact Risks	Consumer Risks
Cross-cutting Risks	Privacy Risks (Interpersonal, Institutional, and Commercial)			
	Advanced Technology Risks (AI, IoT, Predictive Analytics, Biometrics)			
	Risks to Health and Well-being			
Risk Manifestation	Hateful Content	Hateful Behavior	Hateful Encounters	Marketing Risks
	Harmful Content	Harmful Behavior	Harmful Encounters	Commercial Profiling Risks
	Illegal Content	Illegal Behavior	Illegal Encounters	Financial Risks
	Disinformation	Other Problematic Encounters	Other Problematic Encounters	Security Risks

Source: OECD, 2021.

Brief explanations of these categories are provided below.

- **Content Risks:** Children's exposure to harmful material containing violence, hate speech, discrimination, or misinformation that is inappropriate for their age and developmental level.
- **Contact Risks:** Harmful interactions with malicious adults or peers in online environments, including threats such as cyberbullying, privacy violations, and the sexual grooming of children.
- **Conduct Risks:** Digital behaviors that children engage in intentionally or unintentionally and that may harm both themselves and others as a result of their own actions (for example, participating in cyberbullying or creating or sharing harmful content).
- **Consumer Risks:** The unauthorized commercial use of children's digital footprints, exploitation of their data, hidden in-app costs, and exposure to manipulative algorithmic marketing strategies that are inappropriate for their age.
- **Cross-cutting Risks:** These are multilayered threats that extend across the boundaries of the four main categories and involve multiple risks simultaneously. In particular, digital privacy violations, widespread cyberbullying, and AI-based profiling of children's digital footprints stand out as intersecting risk areas that cannot be reduced to a single category and that undermine both family and child digital safety in an integrated manner.

The OECD's risk framework encompasses risks encountered across digital environments. However, given the particular position of social media within digital technologies, risks arising specifically from social media warrant separate consideration. Social media risks extend beyond exposure to content and may also influence how family members compare themselves, their bodies, their achievements, and their standards of living with others. Exposure to idealized bodies and curated representations of everyday life, particularly on visually oriented platforms, may intensify body dissatisfaction and appearance-focused social comparison among children and young people. Although these relationships are neither automatic nor equally strong for everyone, the platform used, the content followed, individual vulnerabilities, and critical media literacy within the family are important determinants (Fardouly & Vartanian, 2016; Holland & Tiggemann, 2016). Influencer culture may also produce commercialized norms concerning consumption, success, parenting, and the "ideal family life." The blurring of boundaries between advertising and personal recommendation may affect children's and parents' consumption expectations, decisions concerning the family budget, and evaluations of lifestyle. Social media risks, therefore, need to be addressed together with advertising transparency, knowledge of commercial persuasion, financial literacy within the family, and the development of realistic expectations (De Veirman, Cauberghe, & Hudders, 2017).

Another dimension of risk that has emerged in recent years arises from artificial intelligence technologies. In particular, the spread of algorithmic content recommendation systems, generative artificial intelligence tools (e.g., ChatGPT, Gemini), personalized education platforms, and virtual interaction environments has made the balance between digital risks and opportunities more complex. Recent research indicates the rapid adoption of AI among children and young people. A report by the United Nations Children's Fund (UNICEF) found that 67% of young people in the United Kingdom use AI (Innocenti UNICEF, 2025). Recent evidence from the United States also shows that AI use extends beyond education and information-seeking. At the same time, research involving parents from 19 countries found that many parents were not fully aware of how their adolescent children were using generative AI and felt disconnected from them on this issue (Eira et al., 2025).

AI systems have the potential to influence children's cognitive, emotional, and social development (Innocenti UNICEF, 2025). As these autonomous systems influence children's patterns of interaction and decision-making processes, significant protection needs arise from the perspective of children's rights. AI systems pose serious concerns regarding data privacy, age-inappropriate manipulation, and algorithmic discrimination. Commercial AI systems that do not take children's developmental needs into account at the design stage risk treating children merely as sources of data. Designing AI technologies through a child-centered, safe, fair, and explainable approach has therefore become an important area of policy attention (Innocenti UNICEF, 2025).

At the same time, the effects of AI on the family institution should not be reduced solely to children's use of it. AI companions and social chatbots can create a sense of continuity, being understood, and emotional closeness among users, and some users describe these systems as friends or confidants (Turkle, 2006; Brandtzaeg, Skjuve, & Følstad, 2022). Although this may provide temporary support for individuals experiencing loneliness, the management of emotional relationships by a commercial platform requires careful consideration regarding personal data privacy, manipulative design, and potential effects on family communication.

Parents' use of AI-supported advisors for child-rearing, health, discipline, education, and family disagreements may also introduce a new form of "algorithmic authority" into family decision-making. These tools may facilitate access to information. However, they may not always adequately account for context, cultural differences, children's developmental characteristics, and the distinctive nature of family relationships. AI outputs should therefore be treated as supportive inputs whose sources and limitations are critically examined, rather than as final decisions that replace professional and parental judgment.

These emerging risks have implications not only for individual safety but also for value transmission within families and broader understandings of social responsibility. The speed of technological change may also create differences in digital knowledge and experience within families, while inequalities in digital access and skills remain closely linked to socio-economic circumstances (UNICEF Innocenti, 2025). Recent evidence also points to a growing AI usage gap within families. Across ten countries surveyed by UNICEF, children were more than three times as likely as their parents or caregivers to use AI systems, highlighting the need to strengthen AI literacy and support within families (UNICEF Innocenti, 2026). Evidence from a recent systematic review and meta-analysis also indicates that digital safety interventions for parents can strengthen parental knowledge and skills and contribute to reductions in children's screen time (Zgambo et al., 2025). In the age of AI, however, parental guidance also needs to address emerging issues such as AI literacy, data privacy, algorithmic awareness, and critical engagement with AI systems.

More broadly, the growing integration of digital technologies into everyday family life affects several interconnected areas:

- **Family Relationships and Communication:** Digital technologies can help family members maintain communication and relationships across distance, while also changing patterns of everyday interaction and the ways family members spend time together.

- **Privacy and Personal Boundaries:** The growing presence of connected devices, platforms, and digital services in family life raises concerns relating to privacy, personal data, children's digital footprints, and personal boundaries.

- **Parenting and Family Responsibilities:** Parents and caregivers increasingly need to guide children's digital engagement, address privacy and safety concerns, evaluate online information, and respond to emerging digital risks.

- **Differences in Families' Digital Experiences:** Families experience digital transformation differently depending on factors such as digital access and skills, socio-economic circumstances, and the availability of appropriate information, services, and support.

The main opportunities offered by digital technologies for family and child well-being, the risks accompanying them, and the related value-based considerations are summarized in Table 2.2.

Table 2.2 Main Digital Opportunities and Risks for Family and Child Well-Being from a Value-Based Perspective

Area	Main Opportunities	Main Risks	Focus of the Value-Based Approach	Related Islamic Values
Communication and Family Bonds	Staying connected with family members living at a distance, care coordination, and mutual support	Disrupted communication, fragmented attention, pressure to remain available, and reduced shared time	Balance between online connection and face-to-face closeness	Hifz al-Usra, Wasatiyyah
Education and Development	Access to learning resources, school-family communication, and parental involvement	Digital divide, commercial data collection, distraction, and low-quality content	Reliable, age-appropriate, inclusive, and privacy-protective learning	Hifz al-'Aql, Amanah
Health and Family Support	Telemedicine, online counseling, early referral, and access in rural areas	Privacy violations, incorrect or incomplete guidance, data security, and unequal access	Privacy-protective, reliable, and harm-reducing health services	Haya, Amanah
Social Media and Entertainment	Creativity, peer support, cultural sharing, and belonging	Social comparison, body image pressure, cyberbullying, and consumerist influencer culture	Truthful, moderate, and respectful participation in digital environments	Adab, Sidq, Wasatiyyah
Artificial Intelligence and Data-Driven Services	Personalized support, accessible information, and administrative convenience	Emotional dependence, algorithmic steering, bias, surveillance, and over-reliance on AI in family decision-making	Human oversight protection of privacy, and the best interests of the child	Hifz al-'Aql, Mas'uliyyah, Hifz al-Nasl

Source: Created by the Authors.

2.4. Transformation of Family Values in Digital Environments

Digitalization is not a one-way process that eliminates family values; rather, it transforms the environments in which values are transmitted, discussed, and reinterpreted. Value transmission no longer proceeds solely from parent to child, as children's digital knowledge and experiences also influence family decision-making. Digital technologies thus have a bidirectional mediating effect in the process of value transmission. Mutual learning between parents and children need not weaken parental authority; rather, it may require authority to rest not merely on technical knowledge but also on trust, consistency, ethical judgment, and the quality of relationships (Livingstone & Blum-Ross, 2020). This reinforces the central position of family cohesion in assessing digital transformation. Trust within the family, emotional bonds, shared family time, a sense of belonging, and intergenerational solidarity are influenced not only by the amount of technology use but also by how technology is integrated into family routines.

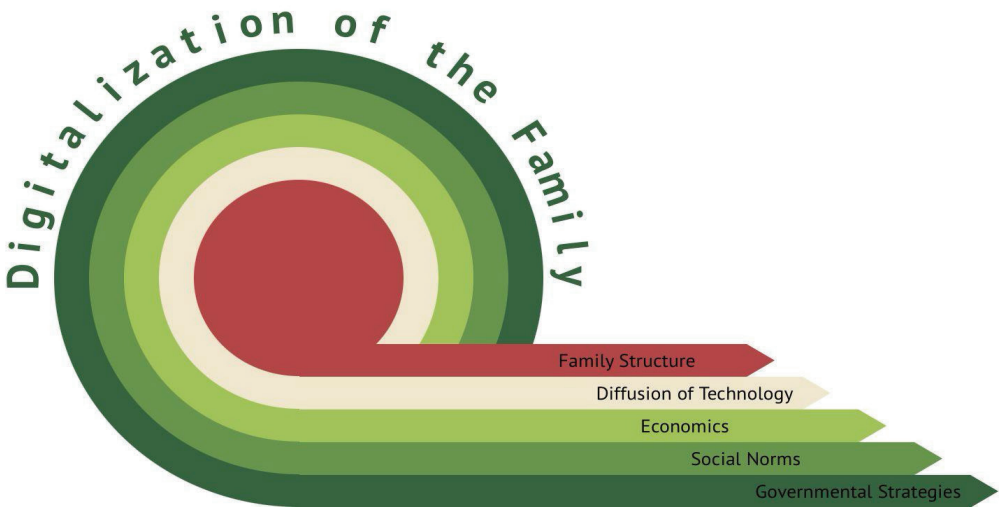
While shared digital activities and communication with relatives living at a distance can strengthen family bonds through digitalization, interrupted conversations, constant notifications, and individualized media consumption may challenge family boundaries and roles (Carvalho, Francisco, & Relvas, 2015).

From a governance perspective, the digitalization of the family is often addressed through protective measures such as legal regulation, technical filtering, and platform-based monitoring. Although the family is an important social environment in which digital interactions take place, the role of families may receive less attention in regulatory processes focused primarily on governments, platforms, and other institutional actors. Current recommendations concerning digital society point to a framework of shared responsibility among governments, the private sector, civil society organizations, and families (OECD, 2021). In addition to being the first environment in which children learn to distinguish right from wrong and internalize moral principles, the family is also the fundamental structure in which they acquire critical digital values such as digital privacy and online etiquette. Ensuring that families are adequately considered and supported in this transformation can therefore strengthen policies aimed at addressing digital risks to children and society.

The transformation of family values in digital environments is best understood as a shift in the conditions under which values are learned, negotiated, and practiced. Platforms influence visibility, attention, social comparison, and communication norms; families in turn interpret these influences through existing relationships and expectations. The analysis below therefore focuses on concrete value-relevant outcomes - privacy, authority, responsibility, truthfulness, moderation, and intergenerational communication - rather than attaching a separate ethical label to each digital practice.

The digitalization of family life does not take place in isolation. Families engage with digital technologies within a broader environment shaped by access to technology, economic circumstances, social and cultural conditions, and public policies and institutional arrangements. These factors influence the opportunities available to families, the digital risks they encounter, and their capacity to use digital technologies safely and meaningfully. At the same time, families differ in their needs, resources, digital skills, and patterns of technology use, meaning that the effects of digitalization are not experienced equally across households (UNICEF Innocenti, 2025). Figure 2.2 brings these influences together under four interrelated factors that shape the digitalization of family life.

Figure 2.2 Factors Affecting the Digitalization of the Family



Source: Created by the Authors.

- **Diffusion of Technology:** Digital technologies constitute the infrastructural layer that enables new forms of interaction and organization within and beyond the family. Information and communication technologies, platforms, and mobile services facilitate communication, financial transactions, parenting tools, and the digital coordination of household tasks. They also give family communication and interaction new temporal and contextual forms. At the same time, the growing use of digital technologies in everyday family life raises issues related to personal data, privacy, and digital safety.

- **Economics:** Economic forces shape both digital access and the ways families incorporate digital technologies into everyday life. Consistent with the concept of the platformization of the family, companies develop digital platforms, applications, and services for use in family life. As a result, some aspects of families' emotional and domestic practices may become commercialized or incorporated into data-driven business models. A family's socioeconomic status can influence its digital access and opportunities to develop digital skills. In a cyclical process, markets drive technological innovation, such as surveillance systems, and these innovations in turn affect family life.

- **Social Norms:** Norms and values influence how families understand and justify digital practices. Cultural expectations can shape what is considered acceptable digital behavior and how families approach children's use of digital technologies, privacy, and online interaction. Digital life within the household, such as children's digital privacy, is also shaped by community norms. Online communities offer families new opportunities for information exchange and peer support.

- **Government:** Public institutions provide the regulatory and institutional framework that shapes digital ecosystems. Public action determines how digitalization is integrated into broader social systems. Government regulation includes policies addressing privacy, data protection, child safety, and platform accountability. Governments also play an important role in public investment in digital connectivity, digital literacy programs, and digital public services. Governments can also promote greater coherence across relevant policy areas while addressing inequalities in digital access and capabilities.

2.4.1. Shifting Norms Around Privacy, Authority, and Responsibility

Privacy, authority, and responsibility are not separate legal issues. They are interconnected components of decision-making in the lives of digitalizing families. The data a platform collects determines privacy; the recommendations and restrictions it generates based on that data shape authority; and the question of who is answerable for resulting harm or inequality determines responsibility. Positioning families merely as "consenting users" within this chain does not provide adequate protection, particularly where children are concerned. This broader shift from reliance on individual consent toward greater organizational accountability also raises questions about institutional access to data and public trust (Austin, 2020). These issues can be considered across three interrelated dimensions:

2.4.1.1. Privacy and the Reconfiguration of Family Boundaries

- **From Individual Consent to Organizational Accountability:** Historically, data privacy has relied heavily on a "notice and consent" model that places responsibility on individuals to read lengthy terms and conditions. Today, global regulatory frameworks such as the European Union's (EU) General Data Protection Regulation (GDPR) and the OECD Privacy Guidelines and related international privacy principles increasingly emphasize data responsibility and organizational accountability.

- **Privacy by Design & Default:** Regulatory frameworks increasingly encourage or require organizations, depending on the applicable legal framework, to embed privacy safeguards into system design and adopt privacy-protective default settings.

- **Shifting the Burden:** Individual consent based on lengthy and complex terms of use makes it difficult for families to assess whether excessive amounts of data are being collected. Platforms and data controllers, therefore, need to meet obligations such as data minimization, privacy-protective default settings, and safeguarding the best interests of the child. At the same time, supporting families with understandable information and accessible mechanisms for objection and remedy can serve an important balancing function.

2.4.1.2. Authority, Autonomy, and Algorithmic Influence

- **Decentralization vs. Centralization:** Authority to manage and protect data is subject to tension between decentralization, which empowers individual users and internal organizational teams, and centralization, which relies on governance structures and state access.

- **State Access vs. Human Rights:** Although governments use data for national security and public safety, changing norms are placing limits on such access. International instruments such as the OECD Declaration on Government Access seek to ensure that state surveillance is consistent with democratic values and human rights (Karjalainen, 2022).

2.4.1.3. Responsibility and Accountability Across the Digital Ecosystem

- **Moving towards a Proactive Duty:** Effective accountability extends beyond formal legal compliance and includes operational tools that support responsible decision-making.

- **The Compliance Gap:** Organizations increasingly need mechanisms to assess their data practices and maintain transparent risk-management frameworks.

- **Social and Ethical Responsibility:** The responsibility of developers, platforms, and public institutions extends beyond minimum regulatory compliance. Anticipating differentiated effects on families and children, conducting impact assessments for high-risk design choices, ensuring transparency, and establishing accessible avenues for redress when harm occurs constitute the operational dimensions of ethical responsibility.

Digital family governance does not treat the family as an end user solely responsible for protecting itself. Instead, it defines an architecture of shared responsibility among platform obligations, public oversight, and families' digital capacities. Assigning responsibility for digital services solely to families is neither fair nor effective. Platforms have responsibilities for designing and operating services in accordance with applicable safety and regulatory requirements, with due consideration for family and child well-being. Public authorities are responsible for ensuring basic access, establishing clear safety standards, creating effective oversight mechanisms, and providing systematic digital literacy and guidance services in schools. Families, in turn, are responsible for relationship-based guidance, value transmission, and role modeling. The shared-responsibility model aims to manage risks across the design, provision, and use stages (International Telecommunication Union, 2020; OECD, 2022).

Privacy in digital family life is not merely an individual preference. Children, parents, and older family members who share devices generate interconnected data trails through school, health, social assistance, banking, and platform services. A post made by one family member may therefore reveal the location, health information, economic situation, or social relationships of other family members. General Comment No. 25 of the United Nations Committee on the Rights of the Child requires that children's privacy be protected based on their evolving capacities and best interests, and that data-processing practices be explained to children in age-appropriate and understandable ways (Committee on the Rights of the Child, 2021).

Protecting privacy within the family requires a balanced approach between parents' protective role and children's evolving autonomy. Although parental monitoring can be used for safety purposes, constant and disproportionate surveillance may weaken children's relationships of trust, willingness to seek help, and expectations of privacy. Age-appropriate rules, clear explanations for monitoring, consideration of the child's views, and gradual relaxation of controls as capacity increases provide a concrete application of Haya, Amanah, and Wasatiyyah: privacy and dignity are protected, parental stewardship remains visible, and protection is kept proportionate rather than becoming continuous surveillance.

Relationships of authority are also becoming multi-actor arrangements because of platforms and algorithmic systems. Parents and teachers are among the actors influencing what children watch and encounter, while recommendation systems, content creators, and advertising technologies increasingly shape everyday choices. This requires not simply expanding parental authority through technical control, but developing a form of guidance that can explain algorithmic influence, encourage children to question sources, and strengthen children's decision-making capacity (OECD, 2024; UNICEF Innocenti, 2025).

This approach treats parental responsibility and children's evolving autonomy as complementary rather than mutually exclusive. The policy objective is to enable families to protect children while preserving trust, privacy, communication, and age-appropriate participation. The framework in Section 1.5 therefore functions here as a proportionality test: responsibility must be real, but protective measures also need to remain context-sensitive and no more intrusive than the risk warrants.

2.4.2. Global Digital Culture, Content Flows, and Tensions with Traditional Values

Digital culture and global content flows are reshaping social interaction by reducing the significance of geographical distance, accelerating real-time information exchange, and increasing interaction between local traditions and global media. While this connectivity can amplify the voices of groups underrepresented in the digital public sphere, it also poses challenges, including algorithmic echo chambers, cultural hybridization, and rapid shifts in digital identity. The interaction between modern digital culture and global content flows shapes everyday life and social development across multiple interconnected dimensions (Alsaleh, 2024). Alsaleh explains this interaction through the following dimensions:

- **Technological Determinism vs. Cultural Agency:** Technologies are shaped by cultural values and practices while also influencing cultural behavior and identities. This theme critiques technological determinism by emphasizing the active role of culture in technological development and adoption.

- **Cultural Adaptation and Hybridization:** Cultures adapt to and modify new technologies, producing hybrid forms of cultural expression that combine traditional practices with modern innovations. This process reflects the dynamic and continuous negotiation between the local and the global.

- **Digital Divide and Cultural Hegemony:** Digital technologies can contribute to or challenge cultural inequalities, particularly regarding access, representation, and power. This dimension examines how the digital divide deepens cultural exclusion and reinforces existing power structures.

Families' engagement with digital culture need not be framed as a binary choice between completely rejecting global content and accepting it uncritically. Rather, families can engage critically with digital transformation while preserving their cultural references and values, interpreting content in context, and developing shared processes of meaning-making with children.Tensions may arise when deeply rooted cultural norms such as community cohesion, respect for elders, and embodied notions of privacy interact with the speed, anonymity, and global reach of digital environments. As digital technologies become increasingly embedded in family life, families may need to reconcile established values and practices with new forms of communication, connection, and digital participation (Livingstone & Blum-Ross, 2020). This interaction is reshaping how families communicate, work, and interpret social reality.Managing the tension between traditional values and digital practices requires addressing the principal areas of conflict and adaptation:

- **Community versus Individualism:** Traditional family and community settings may place greater emphasis on collectivism, mutual assistance, and face-to-face rituals, while some forms of digital engagement may shift attention toward more individualized virtual spaces. From a policy perspective, this tension calls for consideration of how digital environments can support individual participation while also sustaining family and community relationships. (Nishma Bharadia, 2026).

- **Privacy versus Data Sharing:** The cultural norm of keeping personal or community matters private can come into tension with data collection, sharing, and monetization practices in digital environments. Protecting individuals' privacy safeguards their security, dignity, and other fundamental rights and freedoms, including freedom of thought and expression. Although the use of personal data through digital technologies offers significant social and economic benefits, it may also endanger privacy (OECD, 2026).

- **Preservation versus Dilution of Culture:** Although the internet may provide a democratic means of documenting endangered traditions and sharing them globally, popular digital platforms also risk homogenizing cultures and diluting the distinctive meanings of local practices (Siliutina et al., 2024). Cultural dilution occurs when local traditions lose their distinctive qualities or strength under the pressure of pervasive external influences. Communities, therefore, need to develop ways to adapt to global transformations while preserving their cultural distinctiveness.

The policy significance of these tensions is not that global digital culture is uniformly incompatible with family values. Rather, platform incentives and content flows can amplify some practices while weakening others, creating context-specific pressures on privacy, authority, truthfulness, and family interaction. Digital family governance consequently requires both family capacity and institutional safeguards so that cultural and ethical concerns are addressed through transparent, proportionate, and rights-aware mechanisms rather than blanket restriction.

The relationship between global content flows and traditional values should not be reduced to a one-way narrative of "value loss." Digital platforms also enable families to produce religious and cultural content, maintain ties with their roots, increase the visibility of local languages, and record intergenerational memory. At the same time, these environments may circulate commercialized lifestyles and decontextualized norms with high visibility. This points to the importance of strengthening families' capacity to critically evaluate content, engage respectfully with difference, and sustain local values through creative production.

2.4.3. Implications for Family Cohesion and Intergenerational Value Transmission

The effect of digital culture on family cohesion depends not only on the duration of being online but also on how connectivity is integrated into family routines. Regular communication with family members living at a distance, coordination of care, and shared digital production can strengthen family bonds. Conversely, conversations interrupted by notifications, individualized media consumption, and expectations of constant availability can fragment shared family time. Assessing family cohesion therefore requires attention to relational dimensions such as shared activities, face-to-face communication, emotional availability, and intergenerational support, alongside patterns of digital use.

Intergenerational value transmission can become bidirectional in digital environments. Children bring technical knowledge and contemporary platform culture into the family, while adults contribute ethical judgment, life experience, and contextual evaluation. This mutual learning need not eliminate parental authority; rather, it can reconstruct authority around explanation, consistency, and trust. Models in which parents receive technical support from children while children receive adult guidance on source verification, privacy, and responsibility can strengthen families' capacity to engage with digital environments safely and responsibly.

The migration of family rituals into digital environments creates new opportunities for the transmission of values. Online family gatherings, observing religious occasions together, digitally archiving family history, and video calls with elders can support intergenerational continuity. However, these practices should not make family members constantly visible; the rights of children and other family members to control the sharing of their images and personal information, to remain offline, and to define personal boundaries should be respected.

2.4.4. Value-Based Governance Principles for Digital Family Life

The analytical framework presented in Section 1.5 provides the basis for the value-based governance principles discussed below. The six core normative values provide the substantive ethical foundations of the framework: Amanah draws attention to trust and stewardship; Hifz to the complementary protection of the family, progeny, and intellect; Adab and Haya to ethical conduct, dignity, modesty, and privacy; and Sidq to truthfulness and information integrity. Amr bil Ma'ruf wa Nahy'an al-Munkar supports the promotion of beneficial practices and the prevention of wrongdoing, while Wasatiyyah emphasizes balance and moderation. The cross-cutting guiding principles of Hikmah and Mas'uliyyah provide the interpretive and implementation lens, emphasizing context-sensitive judgment, responsibility, and accountability. These principles are applied collectively rather than as separate labels for individual risks.

On this basis, a value-based approach does not mean maximizing control over digital family life. It means designing rules, services, platform safeguards, parental guidance, and remedy mechanisms so that families can benefit from digital opportunities without shifting unreasonable burdens onto parents or children. The practical focus is therefore on shared responsibility, proportionate safeguards, trustworthy information and data practices, family communication, and accessible support when harm occurs.

Five questions can be asked when operationalizing values in any new policy or service:

- What is the intended benefit for the family and the child?
- What are the foreseeable harms and inequalities?
- Which actor bears which responsibility?
- Is there an accessible avenue for objection and remedy for the child and family?
- Through which indicators and mechanisms will outcomes be monitored?

These questions help translate a value-based approach from abstract principles into practical considerations for accountable governance.

2.4.5. Interpreting Risks and Opportunities Through a Value Lens

Interpreting digital opportunities and risks through a value lens requires examining their context-dependent outcomes rather than categorically accepting or rejecting technology. A video-calling application may strengthen care relationships among family members separated by migration; when it creates pressure for constant availability, however, it may weaken family boundaries. An educational platform may offer learning opportunities while also raising privacy and equity concerns through excessive data collection or commercial steering.

A value-based assessment must also account for differences in age, disability-related access needs, household income, geography, language, digital skills, and caregiving circumstances. A measure that is protective for one family may create new exclusion or privacy burdens for another. Hikmah and Wasatiyyah therefore emphasize contextual and proportionate implementation, while Mas'uliyyah highlights institutional responsibility for identifying and addressing foreseeable access and protection barriers. Table 2.3 presents an illustrative framework for applying a value-based perspective to selected digital family policies and services. By linking the expected family benefit, foreseeable risk, relevant values and safeguards, and illustrative outcome indicators, the framework provides a structured way of considering these dimensions together.

Table 2.3 Illustrative Value-Based Framework for Digital Family Policies and Services

Policy / Service Area	Expected Family Benefit	Main Foreseeable Risk	Relevant Values and Safeguards	Illustrative Outcome Indicators
Digital public services	Improved access to health, education, and social support	Exclusion, excessive data sharing, and identity fraud	***Amanah:*** Data minimization, secure access and delegation, and accessible non-digital alternatives	Completion rate by household group; security incidents; user trust
Education platforms and AI tutors	Personalized learning, access to educational support, and school-family communication	Commercial profiling, inaccurate advice, and over-reliance	***Hifz; Sidq:*** age-appropriate design, human oversight, and source transparency	Learning benefit; correction/appeal rate; child well-being
Social media and entertainment	Creativity, participation, and peer support	Cyberbullying, manipulative design, and harmful comparison	***Adab and Haya; Wasatiyyah***: safe defaults, reporting, and digital well-being tools	Reporting resolution; repeated harm; healthy-use indicators
Family communication and connected devices	Care coordination and intergenerational connection	Technoference, surveillance, and loss of private space	***Hifz; Adab and Haya***: shared rules, device-free routines, and proportionate monitoring	Family dialogue; shared time; perceived autonomy
Online health and family support	Remote access to counselling and early help	Misinformation, confidentiality breaches, and unsafe automation	***Amanah; Sidq***: professional standards, confidentiality, source reliability, and referral to human support	Successful referral; confidentiality incidents; satisfaction

Source: Created by the Authors.

Note: In this table, Hifz refers collectively to the protection of the family (hifz al-usra), progeny (hifz al-nasl), and intellect (hifz al-'aql).

3. TRENDS IN FAMILY AND DIGITAL GOVERNANCE: GLOBAL AND OIC PERSPECTIVES

This chapter examines major trends in family and digital governance from global and OIC perspectives. It traces the evolution of policy approaches to the digitalization of family life, reviews emerging regulatory and institutional responses, and examines the implementation mechanisms through which families and children are supported and protected in digital environments. Particular attention is given to the changing distribution of responsibilities among public authorities, digital platforms, institutions, families, and other relevant actors. The chapter also considers the diversity of approaches and capacities across OIC Member Countries, identifying common patterns, implementation challenges, and emerging policy priorities.

3.1. Global Context in Brief: Evolution of Digital Family Governance

The evolution of digital family governance reflects the changing role of digital technologies in family and social life. As digital access, platforms, and connected technologies have become increasingly embedded in everyday activities, policy attention has gradually expanded from questions of access, individual consent, and parental control to broader concerns involving child and family protection, privacy, platform responsibility, and institutional accountability. The following overview traces this evolution from the early commercial internet to the contemporary digital environment and highlights the main shifts that have shaped current approaches to digital family governance.

3.1.1. Late 1990s to 2000s: Market-Oriented and Consent-Based Approaches

In the early years of the commercial internet, governments viewed connectivity more as a societal resource than as a household necessity. Digital inclusion policies focused on connecting public spaces, such as schools and libraries, while leaving household access largely to the free market.

During the same period, many early approaches to digital regulation reflected a relatively libertarian, "hands-off" orientation. Digital rights were often framed primarily through consumer-contract rights. Policymakers viewed the internet as a marketplace and defined the primary right afforded to families as a "right to consent." The emblematic intervention of the period was the United States Children's Online Privacy Protection Act of 1998 (COPPA), which gave parents legal authority to permit or restrict the use of their children's data. From a rights-based perspective, however, this approach created a problematic paradigm (Takhshid, 2023). Treating privacy as a tradable commodity rather than a fundamental human right created a misleading perception of choice. Although families had the "right" to refuse data collection, exercising that choice could mean exclusion from the digital world. This approach placed considerable responsibility on parents to protect their children's privacy in their interactions with technology companies, while providing limited structural support.

3.1.2. 2010s: The Rise of Digital Parenting and Emerging Rights Debates

The spread of affordable broadband internet and smart devices made cyberspace deeply embedded in the family environment. In response, policy shifted toward a market-oriented support model designed to provide discounted internet access to low-income households. The internet became one of the basic infrastructures of everyday domestic life. As mobile devices, smartphones, and tablets became increasingly common, privacy concerns shifted from desktop computers to continuous everyday consumption and connectivity. Governments responded by referring the issue to relevant pediatric and health authorities to develop guidelines on "screen time" (Ponti, 2023). Competent authorities called on parents to adopt an "active mediation" approach and to use restrictive controls to manage digital device use at home. As a result, parents faced a dual challenge: ensuring family access to the internet while also protecting their children from emerging algorithmic and data-collection practices. Another major technological development during this period was the emergence of social media. Combined with the capacity of smart devices for constant connectivity and documentation, social media made previously implicit tensions within the family unit more visible. Some parents embraced these opportunities for freedom of expression, socialization, and even generating income from family life. In the context of digital parenting, the practice known as "sharenting," in which parents share content about their children, generated intense debate about the balance between children's and parents' rights.

These practices brought concerns, including children's involuntary digital footprints, to the forefront. Some stakeholders have defended the right to be forgotten as a fundamental right to an open future.

Rather than treating the digitalization of the family primarily as a product-design or systemic-safety issue, policy approaches during this period often framed it as an individual parenting challenge, giving rise to the concept of "digital parenting" (Benedetto & Ingrassia, 2021). Throughout this decade, legal frameworks provided limited mechanisms to protect children's digital rights from excessive parental sharing, exposing a significant blind spot in traditional family law.

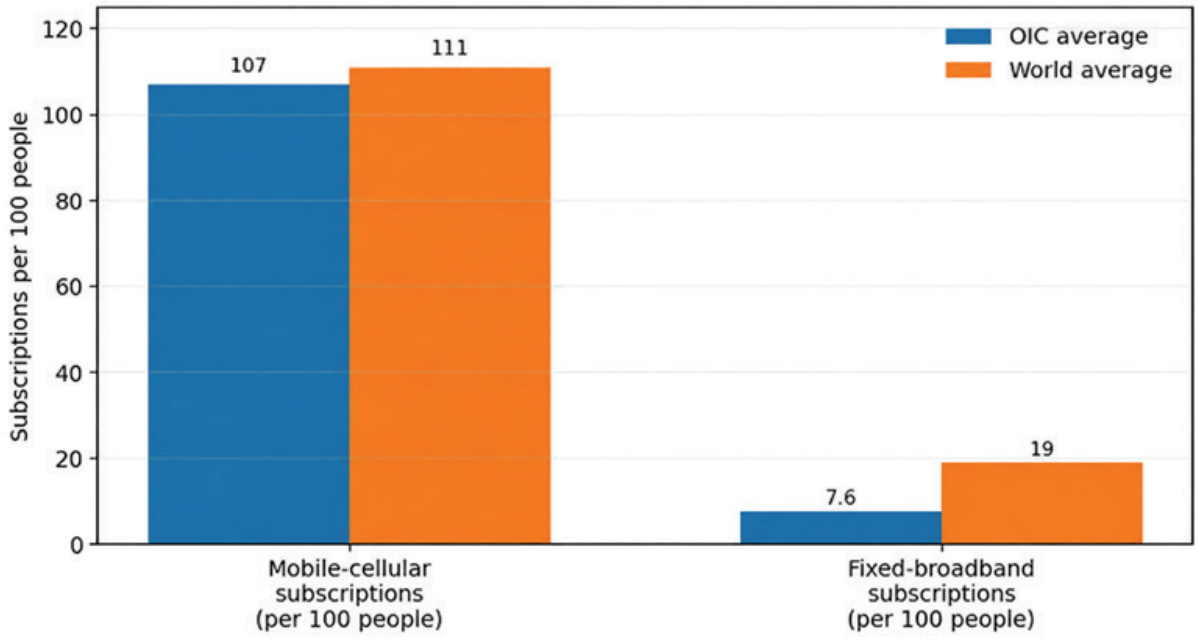
3.1.3. 2020s: The Pandemic Catalyst and the Limits of Individual Consent

The global lockdowns caused by the pandemic made it clear that digital access was no longer optional for many essential activities. Governments therefore introduced large-scale emergency interventions to ensure continuity in essential services, including education, health, and public services. Within a very short period, devices and broadband connections were rapidly expanded or provided to families in many contexts. This rapid change significantly affected digital arrangements at both societal and family levels. Families increasingly relied on commercial educational technology platforms and online examination proctoring software at home, while efforts to ensure the continuity of public services also raised new considerations regarding family privacy.

In the digital age, where access to digital resources has become increasingly important for participation in everyday life, the limitations of relying primarily on traditional models of individual or parental consent have become more apparent. Concerns about family privacy persisted in the post-COVID period as connected technologies became increasingly integrated into domestic life. The spread of smart televisions, robot vacuum cleaners, internet-connected toys, and baby monitors created new possibilities for technology companies to collect and process household data, including home maps, voice recordings, sleep patterns, and daily routines. These developments further highlighted the limitations of individual consent as the primary mechanism for protecting family privacy, particularly where access to widely used digital services depends on accepting standardized terms and data practices.

Although digital connectivity continues to expand across OIC Member Countries, a gap relative to the global average persists particularly in fixed broadband connectivity. According to SESRIC's 2024 Statistical Yearbook, the OIC average in 2023 was 107 mobile-cellular subscriptions and 7.6 fixed-broadband subscriptions per 100 inhabitants. ITU values for the world in the same year were 111 and 19, respectively. As illustrated in Figure 3.1 the convergence observed in mobile connectivity has not occurred to the same extent in fixed-broadband use (International Telecommunication Union, 2023; SESRIC, 2024).

Figure 3.1 Selected Connectivity Indicators: OIC and World, 2023



Source: SESRIC (2024) and International Telecommunication Union (2023).

3.2. Emerging Trends in Family and Child-Centered Digital Governance

Emerging trends in family- and child-centered digital governance increasingly combine four functions: prevention and capability-building; safer platform and service design; accessible reporting and remedy; and evidence-based coordination across institutions. Their relevance to digital family governance lies not in the number of instruments adopted, but in whether these functions collectively reduce avoidable harm, strengthen family capacity, preserve privacy and trust, and keep responsibility proportionate to the power of each actor.

Today, digital rights are increasingly framed in terms of systemic protections rather than individual choices. This shift increasingly recognizes online safety as a systemic issue rather than solely a matter of individual or parental responsibility. Because digital technology has fundamentally changed how families communicate, establish boundaries, and maintain cohesion, leaving regulatory responsibility entirely to parents is increasingly regarded as an unsustainable burden (Bărbuță et al., 2023).

Within this evolving context, a range of issues affecting families and children has come to the forefront:

- The widespread and intensive use of digital technologies weakening communication within the family,
- The effects of AI-based algorithms on social media and gaming platforms on children's intellectual development and processes of addiction,
- The effects on children's safety of deepfake technology, which has become easier to produce through AI and can significantly undermine information accuracy,
- The effects of digital identities created by children in digital games or environments on their mental well-being,
- Commercial digital platforms obtaining and processing children's personal data without parental consent in ways that raise concerns regarding consent, privacy, and data protection,
- The transformation of parenting into "digital parenting" alongside digital technologies and the difficulties parents face in keeping pace with expectations to become digitally literate,

- Conflicts between digital culture and local, family, or Islamic values and the tendency of such conflicts to distance children from these values,

Governments are increasingly moving toward a "best interests of the child" framework. Emerging policy approaches increasingly go beyond telling parents to limit screen time and instead focus on requiring platforms to change their underlying architectures. This period is characterized by comprehensive regulatory frameworks such as the United Kingdom's and California's age-appropriate design frameworks and the EU Digital Services Act (DSA), which require privacy-protective defaults, algorithmic transparency, and product design that incorporates child safety from the outset. These approaches increasingly view the family not as a collection of consumers who must individually read terms of service, but as a social institution whose protection also requires structural and preventive regulation of technology providers.

3.3. Evolution of Regulatory Framework: Global Approaches and OIC Practices

The regulatory comparison below is therefore organized around the policy functions that matter for families: assigning duties to platforms and public bodies, protecting children's and family data, improving information integrity and transparency, providing proportionate safeguards for age-related risks, and ensuring accessible complaint and remedy mechanisms. This functional approach allows the regulatory frameworks to be examined in terms of their practical implications for families and children rather than as a separate inventory of legal instruments.

At the global level, various legal regulations address issues that children may encounter in digital environments, particularly cyberbullying, sexual harassment, psychological abuse, privacy, the safe use of social media, and the use of artificial intelligence. Over time, regulatory frameworks have increasingly incorporated provisions relevant to the protection of children in digital environments as digital technologies have advanced. They establish a legal basis for future practices and require private-sector organizations that provide digital technology services to comply with specified rules.

One of the earlier legal instruments in this evolving regulatory landscape is the United States Children's Online Privacy Protection Act (COPPA). Enacted in 1998 and entering into force in 2000, COPPA imposes specific restrictions on the online collection of personal information from children under 13. In particular, COPPA restricts the collection of personally identifiable information from children without parental consent. The following provisions apply under COPPA (Federal Trade Commission, 2002):

- Websites directed at children that collect personal information, as well as other websites that knowingly collect personal information from children aged 12 and under, must publish a privacy policy;
- Websites must provide information, at every point where personal information is collected, about how information obtained from children will be used and whether it will be shared with third parties;
- Parents must be informed about the website's information-collection and sharing practices and be allowed to opt out on behalf of their children;
- Websites must be required to obtain verifiable parental consent before collecting, using, or sharing information about children or allowing children to create an email account or post messages in a chat room;
- Parents should be permitted to review personal information collected from their children;
- Parents must be allowed to withdraw consent regarding personal information collected from their children and to have that information deleted upon request;
- Websites must be required to establish and maintain procedures to protect the privacy, security, and integrity of children's personal information;
- Websites must not condition children's participation in specific activities on the collection of more personal information than is reasonably necessary.

Building on the growing emphasis on data protection and privacy, another major legal framework is the General Data Protection Regulation (GDPR) established by the European Union.

The GDPR was enacted to protect the privacy and security of personal data. Adopted in 2016 and entering into force on 25 May 2018, the Regulation establishes rules concerning the protection of natural persons about the processing of personal data and the free movement of such data. It also safeguards the fundamental rights and freedoms of natural persons, particularly the right to the protection of personal data. The GDPR requires organizations that offer services to individuals residing in the EU or monitor their online behavior to comply with specified rules. Companies that violate these rules may face substantial fines depending on the severity of the infringement.

In summary, the rights of data subjects under the GDPR include the following (European Union, 2026):

- The obligation of the data controller to provide transparent information, communication, and procedures enabling the data subject to exercise his or her rights (Article 12),
- The information that the data controller is required to provide, regardless of whether the personal data was obtained from the data subject (Articles 13 and 14),
- The data subject's right to obtain confirmation from the data controller as to whether personal data concerning him or her is being processed and, where they are, to access that data and information about the processing (Article 15),
- The data subject's right to obtain without undue delay the rectification of inaccurate personal data concerning him or her and, taking account of the purposes of processing, to have incomplete personal data completed, including by providing a supplementary statement (Article 16),
- The data subject's right to obtain the erasure of personal data concerning him or her without undue delay (the right to be forgotten), and the controller's obligation to erase such data without undue delay when any of the conditions specified in the Regulation apply (Article 17),
- The right of the data subject to request restriction of processing where any of the conditions specified in the Act apply (Article 18),
- The controller's obligation, upon the data subject's request, to inform the data subject regarding the rectification or erasure of personal data or restriction of processing (Article 19),
- The data subject's right to receive personal data concerning him or her that were provided to a controller in a structured, commonly used, and machine-readable format and to transmit those data to another controller without hindrance from the controller to which the data were provided (Article 20),
- The data subject's right not to be subject to a decision based solely on automated processing that produces legal effects concerning him or her or similarly significantly affects him or her (Article 21).

Alongside these developments in privacy and data protection, regulatory approaches have increasingly addressed the broader responsibilities of digital platforms. In this context, the Digital Services Act (DSA) represents another important legal framework. The DSA, adopted by the EU and entering into force in 2022, seeks to regulate the digital sphere, combat online disinformation and illegal content, and protect user rights. The DSA's principal objective is to create a digital environment that respects the fundamental rights of citizens and consumers. It seeks to empower European citizens by strengthening the protection of their fundamental rights online and providing greater control and choice when they use online platforms and search engines. It also specifically aims to minimize the risk of children and young people being exposed to illegal and harmful content. The DSA includes rules for very large online platforms such as Google and Meta; online platforms that connect buyers, sellers, and content creators; providers of cloud storage and web hosting services; and internet service providers that offer intermediary services. Under the DSA:

- Platforms must explain the reasons for removing or suspending content,
- Easy mechanisms must be established for users to report illegal content, and platforms must review and remove such content rapidly,
- Platforms must respond to user reports and provide options to appeal decisions,
- Platforms must implement protective measures for children in their services to reduce exposure to age-inappropriate content such as gambling or pornography,

- Social media platforms must explain the algorithms used to recommend content and provide users with a non-algorithmic (neutral) feed option,
- Advertisements displayed on platforms must be clearly labeled as advertising and must provide information such as who placed the advertisement and why it is being shown,
- Personalized advertisements targeting children should not be displayed,
- Users must not be steered toward unwanted subscriptions or purchases through deceptive interface designs such as aggressive pop-ups or confusing and misleading consent buttons,
- Platforms must verify and display sellers' contact information in marketplaces so that users have clear information about the person from whom they are purchasing goods or services.

The DSA also requires platforms to provide a clear and accessible point of contact that users can easily reach to report problems or complaints (Article 12). It further defines citizens' basic online user rights by enabling users who encounter illegal content, such as child sexual abuse material or counterfeit products, to report that content directly through platform reporting mechanisms (Article 16), and by requiring platforms to clearly communicate content-moderation decisions to all affected users (Article 17) (European Commission, 2026).

A similar emphasis on online safety and platform accountability can be observed in the United Kingdom. The Online Safety Act (OSA), whose scope was expanded in 2023 to strengthen the protection of children and adults online, places greater responsibility on digital platforms for user safety. It requires platforms to take measures against illegal content and activities, prevent children from accessing harmful and age-inappropriate content, and provide clear and accessible channels for parents and children to report online problems. The Act covers a wide range of illegal content and activities, including child sexual abuse and other forms of sexual violence, fraud, racially or religiously aggravated public-order offences, incitement to violence, human trafficking, content encouraging or facilitating suicide, intimate-image abuse, the illegal sale of drugs or weapons, and terrorism (GOV UK, 2025).

Beyond these legal and regulatory frameworks, complementary mechanisms have also been developed to support online safety through reporting, awareness-raising, and international cooperation. One such mechanism is the network of Safe Internet Centers (SICs), which operates in 36 European countries, including EU Member States, the United Kingdom, Iceland, Norway, and Türkiye, under the European Union's Better Internet for Kids program. These centers serve as points of contact for reporting online problems such as cyberbullying and digital abuse. Through various activities and initiatives, Safe Internet Centers seek to improve online safety for children and young people and to provide comprehensive content and services to support them and their families (Better Internet for Kids, 2026). The centers provide services that include at least one of the following components: a Hotline, a Helpline, or an Awareness Center. The Hotline receives and assesses reports of illegal content on the Internet. Staffed by professionals such as psychologists, communication specialists, and information technology experts, the Helpline primarily offers solutions to problematic internet use among children and their families. The Awareness Center provides children, young people, parents, and teachers with information and advice on staying safe online (Bayzan, n.d.). Safe Internet Center Plus (SIC+) is an international program that facilitates cooperation and information sharing between the network of Safe Internet Centers within the European Union and comparable organizations operating outside Europe. Through the program, European standards and best practices on children's cyber safety are shared with countries worldwide to strengthen global cooperation. It also promotes experience sharing to develop joint campaigns and strategies against digital threats such as cyberbullying, illegal content, and child abuse. It supports the preparation of shared awareness materials for children, families, and teachers.

Against this broader global regulatory and institutional landscape, OIC Member Countries have also developed a range of legal and policy frameworks concerning child protection and digital safety. In this context, many Member Countries have national laws or international conventions that protect children's rights. Examples include the Child Protection Law, which entered into force in Türkiye in 1990 and directly protects children; the Child Rights Act adopted in Nigeria in 2003; the Child Protection Policy and Child Welfare Act implemented by the Ministry of Labour and Social Affairs in Iraq; the Children's Rights Law adopted in Jordan in 2022 to protect children from all forms of abuse and exploitation; and the Federal Law on Child Rights (Wadeema) in force in the United Arab Emirates.

With the development and spread of digital technologies, comprehensive legal regulations and policy measures have been introduced to protect children's data privacy in digital environments, address cyberbullying, and strengthen children's online safety. Examples of legal frameworks designed to protect children in the digital sphere include Türkiye's Law on the Regulation of Publications on the Internet, which entered into force in 2007; the Personal Data Protection Law, which entered into force in 2016; and the Action Plan for Empowering Children in the Digital World; Nigeria's National Child Online Protection Policy; Saudi Arabia's Personal Data Protection Law; and Malaysia's Communications and Multimedia Act (CMA). Türkiye is a member of the SIC network operating across the European Union, while Egypt, Morocco, and Pakistan participate within the expanded SIC+ framework. Participating countries seek to ensure the online safety of children and young people through various activities and initiatives, and provide comprehensive content and services to support children, young people, and their families. In recent years, steps have also been taken to introduce age restrictions on social-media use in order to protect children's mental health. In Indonesia, for example, social media platforms are required to implement age-verification systems that prevent children under 16 from opening accounts without parental consent and supervision.

The legal frameworks, policy measures, and supporting mechanisms discussed above provide a broader basis for identifying common areas of intervention in digital family and child governance. Against this background, regulatory frameworks can be grouped around five main themes. These are platform duties of care, protection of children's data, age-appropriate design, accessible reporting and remedy mechanisms, and strengthening families' digital capacities. This suggests that effective digital family and child governance generally requires more than a single piece of legislation. Regulations are more likely to succeed when they combine a clear allocation of responsibility, independent oversight, accessible avenues of redress for families, design standards that safeguard the best interests of the child, and indicators that monitor implementation outcomes.

While global regulation is increasingly shifting responsibility from individual parental consent to systemic obligations on platforms and data controllers, OIC Member Countries exhibit marked differences in the scope of legislation and implementation capacity. Across different national contexts, an important consideration is therefore how regulatory frameworks are connected with institutional implementation, service capacity, and mechanisms for monitoring outcomes.

As summarized in Table 3.1, regulatory frameworks can be grouped around five main themes: platform duties of care, protection of children's data, age-appropriate design, accessible reporting and remedy mechanisms, and strengthening families' digital capacities.

Table 3.1 Global Regulatory Approaches and Implications for the OIC Context

Regulatory Area	Main Global Approach	Function for Families and Children	Implication for the OIC Context
Platform and Content Governance	Risk-based platform obligations such as the DSA and OSA	Increases platform responsibility for harmful content, manipulative design, advertising, and reporting processes	National-law definitions of comparable obligations need to be accompanied by effective oversight capacity and cooperation with platforms
Personal Data and Child Privacy	GDPR, COPPA, and national data protection laws	Provides protection through data minimization, transparency, parent/child rights, and safeguards concerning automated decisions	General data-protection provisions should be specified concretely for children's data, intra-family sharing, and AI applications
Age-Appropriate and Safe Design	Privacy by default, age assurance, restrictions on targeted advertising	Shifts the burden of protection from the end user to service design	Technical age assurance should be assessed together with risks to privacy, access, and non-discrimination
Reporting, Assistance, and Referral	SIC, hotline, and helpline models	Provides families with legal, psychosocial, and technical support and facilitates the removal of harmful content	Adoption of a model that integrates safe-internet service provision with social services, law enforcement, and victim support
Digital Capacity and Prevention	School-family education, media literacy, and parenting programs	Strengthens families' capacity to recognize risks, communicate, and seek help	Preference for continuous programs adapted to age and local context rather than short-term campaigns

Source: Authors' compilation based on Federal Trade Commission (2002), European Union (2026), European Commission (2026), GOV.UK (2025), Better Internet for Kids (2026), and Bayzan (n.d.).

3.4. Models of Institutional Governance: Structures and Coordination

Institutional governance determines whether regulatory commitments become a coherent experience for families. From the report's analytical perspective, the central issue is not whether governance is formally centralized or decentralized, but whether responsibilities are clear, complementary, coordinated, and accountable across the institutions that handle education, child protection, data, cybersecurity, communications, social services, and digital transformation.

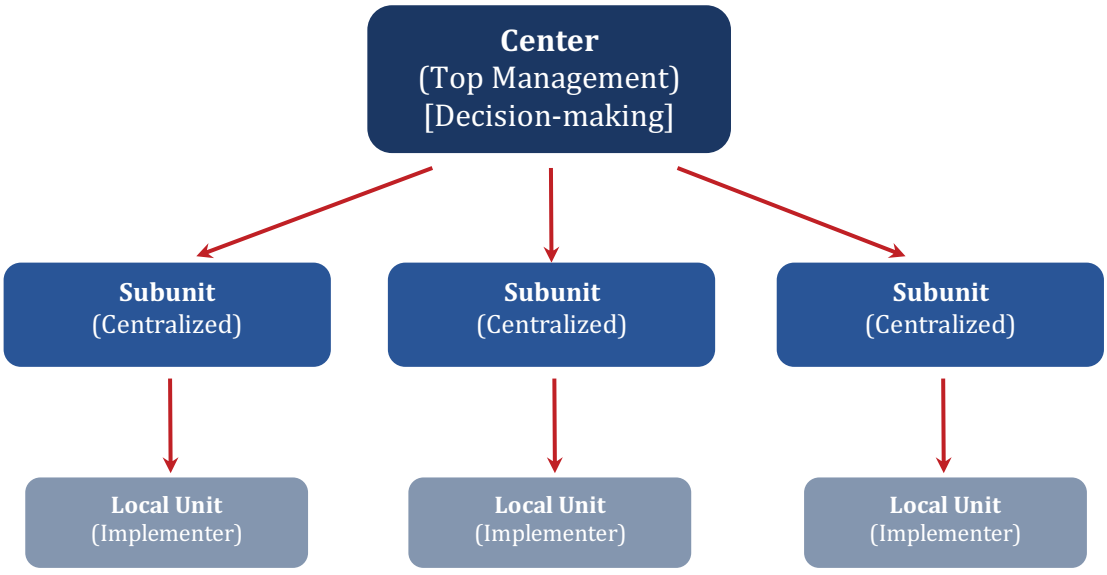
When institutional governance models are examined through the lens of digital family governance, centralized, decentralized, and hybrid models can be distinguished (Virtue & Rainey, 2015). These models differ in the distribution of authority, responsibility, and decision-making power. Forms of coordination among the institutions included in each governance model also vary.

In the centralized governance model, authority for decision-making and for determining policies and strategies is vested in a single central institution. The institution with decision-making authority establishes standards, defines policies, and oversees implementation processes in the relevant area. Policy, decision-making, and administrative functions concerning general public services are carried out by units under the direction and oversight of the central government. The governance process has a top-down structure. Decisions are taken centrally and transmitted to subordinate units for implementation. Thus, all decisions taken by senior managers are implemented by lower-level managers (Figure 3.2). The advantages of this system include the following:

- It helps ensure consistency and coherence in policies, practices, and decisions. Centralizing authority at the senior-management level promotes alignment between policy and implementation,
- Taking decisions from a single source facilitates the operation of subordinate units,
- Strategic plans can be developed and implemented within a unified institutional framework,
- It prevents unnecessary duplication of resources (funding, personnel, etc.) and efforts directed toward the same objective,
- Because strategic plans are developed by senior management, confidence in these plans and the likelihood of success increase,
- In emergencies, rapid decisions binding all units can be taken,
- The organization's overall objective is kept in view at all times.

However, in this model, subordinate units find it difficult to act independently, and centralized approval processes may slow operations. Requiring all approvals to pass through senior management may also create time-management problems at the upper levels.

Figure 3.2 Centralized Governance Model



Source: Created by Authors.

In the decentralized governance model, authority, responsibility, and decision-making power are distributed among different institutions rather than concentrated in a single central institution. In other words, decision-making authority is delegated from senior management to lower-level managers. Different institutions establish their own policies, procedures, and processes for developing and implementing strategies in the relevant area. Rather than a single lead organization, the model relies on inter-institutional cooperation and coordination. Subordinate units are given the freedom to act and make decisions, enabling them to develop plans for their own areas of responsibility (Figure 3.3).

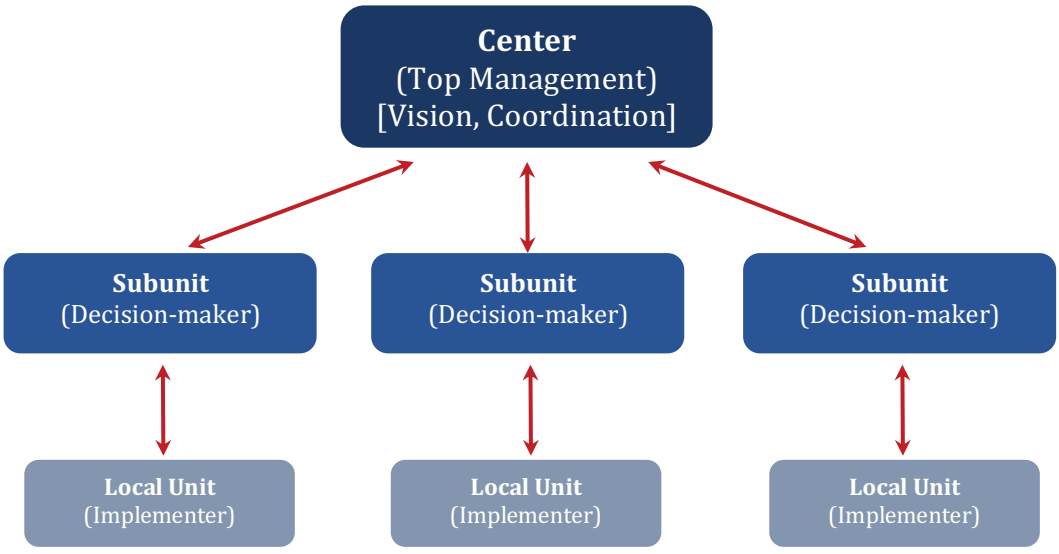
The advantages of the decentralized governance model are as follows:

- Decision-making, communication, and management activities can be carried out more efficiently., particularly where local responsiveness is important,
- Delegating decision-making authority to lower-level managers makes it possible to benefit from their skills,
- Because every decision does not require approval from senior management, savings in time, effort, and cost can be achieved,

- As senior management's workload is shared, it can focus on long-term strategies rather than day-to-day operational matters.

However, in this model, differing practices among subordinate units may lead to inconsistency and insufficient oversight. The independent operation of each unit makes it more difficult for the central body to monitor and supervise all processes. Independent work by different departments may hinder interdepartmental communication and lead to service overlap. Subordinate units may compete with one another by focusing on their own success rather than shared organizational goals. In addition, delegation of authority may create accountability challenges where responsibilities and decision-making mandates are not clearly defined.

Figure 3.3 Decentralized Governance Model



Source: Created by Authors.

The hybrid governance model combines centralized and decentralized governance, establishing a balance between the two. It therefore brings together the strong oversight and standardization advantages of the centralized model with the speed, flexibility, and local-adaptation advantages of the decentralized model. In hybrid governance, which integrates elements of both models, authority, responsibility, and decision-making power are shared between a central institution and other institutions. The central institution develops strategy, defines policies, and sets standards. In contrast, other institutions establish procedures and processes within their own areas in ways that contribute to the defined core strategies and policies. In particular, the central authority answers the question "What should we do?" on matters such as institutional vision, budget constraints, and priority objectives, whereas the answer to "How should we do it?"—covering matters such as the selection of managers, local implementation, and process management—is largely left to subordinate units. Although these units have freedom of action, they may not operate outside the legal and administrative framework established by the central authority. Their success or failure is measured against performance indicators and standards defined at the central level (Bektaş, 2018; Genç, 2012; Koçel, 2020; SNOWFLAKE, 2026; Virtue & Rainey, 2015).

Institutional arrangements may also become fragmented when decision-making, policy implementation, and oversight are distributed across numerous institutions without effective coordination. In such cases, the governance structure may not be clearly defined. Although flexibility granted to institutions may increase efficiency, coordination problems may arise among them.

Different institutional arrangements can be observed in practice, ranging from structures led by a central institution to models involving cooperation among multiple public bodies, private-sector actors, and civil society organizations.

In the United Arab Emirates, the "Digital Quality of Life Council" makes decisions aimed at protecting Emirati society from digital risks and content inconsistent with traditional customs, preserving family-centered moral, social, and cultural values consistent with Islamic teachings, and strengthening the capacity of new generations to cope with digital challenges (Ministry of Interior of the United Arab Emirates, 2024). In Singapore, the Digital Government Directorate under the Ministry of Finance (MoF), the Government Technology Policy unit of the Ministry of Communications and Information (MCI), and the Smart Nation Program Office (SNPO) under the Prime Minister's Office were brought together in 2017 to establish the Smart Nation and Digital Government Office (SNDGO), to provide more integrated digital-governance processes. Singapore's "Digital for Life" initiative, launched to build an inclusive society during its digital transformation, is also implemented in cooperation with 267 private-sector organizations (Digitalforlife.gov.sg). In Kazakhstan, the "Digital Family Card (DFC)" program is implemented by the United Nations Development Programme (UNDP), the Ministry of Labour and Social Protection, and the Ministry of Digital Development, Innovation and Aerospace Industry. Developed to improve the quality of life through data-based decision-making using digital technologies, the program facilitates access to social assistance for all families. Data obtained from public institutions are used to create a digital profile for each family, and real-time data on family structure, income, and social circumstances support the equitable distribution of social assistance (ITU, 2023; Mukhamedkaziy, Maratova & Mustafin, 2025; Zehir & Odabaşı, 2025). In Türkiye, the "Safe Internet Center" was established in 2017 within the Information Technologies and Communication Authority (BTK). Operating with a sense of social responsibility, the Center organizes training sessions, seminars, conferences, symposia, workshops, and other activities and shares open-source content to help internet users—especially children and young people—use internet technologies more consciously and effectively (Güvenli İnternet Merkezi, 2026).

3.5. Implementation Mechanisms and Policy Instruments

Implementation mechanisms translate regulatory and institutional arrangements into practices that families and children can actually use. The mechanisms reviewed below are therefore assessed by function - capability-building, safe design and technical protection, community outreach, and reporting/support - and by whether they connect prevention to remedy. This approach avoids treating program activity as evidence of success in itself.

In practice, these mechanisms range from education and family-support programs to technology-based protection tools and reporting services.

3.5.1. Capacity Building and Field Delivery of Family-Support Services

Formal and non-formal education programs are organized to help families and children acquire comprehensive knowledge about digital technologies and interact with the digital world in healthy ways. Digital literacy and digital citizenship courses are increasingly incorporated into education systems so that children can develop digital literacy skills from an early age and use technology responsibly, ethically, and safely. In Qatar, for example, primary-school curricula include lessons on internet safety, online privacy, and respectful online behavior. As students progress through grade levels, topics such as digital footprints, cybersecurity, and the legal dimensions of online behavior are addressed at more advanced levels (Al Wahaibi, Al-hijji, & Raja Hussain, 2025). South Korea implements a comprehensive digital citizenship program that covers key topics such as privacy management and mechanisms to detect and prevent cyberbullying (Lee, 2023). In Türkiye, lower-secondary courses such as "Media Literacy" and "Information Technologies and Software" provide education on cyberbullying, safe internet use, access to accurate and reliable information, ethical values, digital citizenship, privacy, and security (Ministry of National Education, 2018a; Ministry of National Education, 2018b). Education and certification programs are also organized to help parents develop digital literacy skills. Singapore's "Digital for Life" initiative, launched in 2021 to bring the public and private sectors together and support Singapore society in embracing digital transformation, aims to strengthen digital literacy skills. Public institutions and numerous private-sector organizations support the initiative. It carries out activities to protect individuals from negative experiences in digital environments, such as harassment, cyberbullying, and fraud, while preparing them for the future by strengthening their digital skills. It also supports children and young people in using online environments safely and helps parents acquire the skills needed to guide their children's use of digital technologies. In this context, it offers resources adapted to different developmental age groups. It organizes workshops and online seminars to help parents better understand their children and the digital world (Digital for Life, 2026).

3.5.2. Safe Design, Age Assurance, and Technical Protection Tools at the Family Level

Various software tools, including safe internet filters, screen-time management tools, and monitoring tools, can support the safe use of digital technologies. AI-based filtering or age-assurance systems embedded in digital platforms or offered by internet service providers can also help protect children, in particular from harmful content they may encounter online. Wider use of features such as safe-search options in search engines, blocking age-restricted videos on video-sharing platforms, and sensitive-content filters on social media can likewise help protect families and children from harmful or age-inappropriate content.

For example, the Safe Internet Service, launched in Türkiye in 2011, is provided free of charge on request by internet service providers, helping to protect children and families from harmful online content. The Child Profile provides access to a wide range of useful websites offering approved content in areas such as education, culture, arts, business, economics, homework, banking and finance, careers, shopping, health, music, news, email, public institutions, travel, private companies, educational institutions, and e-government. In addition to the Child Profile, the Family Profile provides access to personal websites, forums, and social-media sites (Information Technologies and Communication Authority, 2019). In Singapore, the "Parenting for Wellness" website, developed through cooperation among the Health Promotion Board, the Ministry of Education, and the Ministry of Social and Family Development, provides resources that help parents build stronger relationships with their children, understand how to support their children's mental health and emotional well-being, and practice effective parenting in the digital age. Through the site, parents can access modules and tools covering topics such as strengthening the parent-child relationship, understanding the digital environment, effectively managing children's use of digital technologies, and guiding children in coping with online harms and risks (Parenting for Wellness, 2026).

3.5.3. Awareness, Community Outreach, and Local Partnership Mechanisms

Nationwide campaigns or projects can provide awareness-raising and support mechanisms to protect families from risks posed by digital technologies. For example, the "Protect Children Online" (CYBER TUMAR) awareness campaign was launched in 2024 through a partnership between UNICEF Kazakhstan and the Committee for the Protection of Children's Rights of the Ministry of Education of the Republic of Kazakhstan. The campaign focuses on major online threats, including cyberbullying, content that is inappropriate or prohibited for children, digital risks to children's safety and privacy, and internet addiction during childhood. A range of informational tools was developed as part of the campaign, including social media posters, materials containing practical advice from experts, and educational videos (UNICEF Kazakhstan, 2024).

In Albania, hundreds of "Smart Labs" were established in schools across the country under the Digital Education Project implemented between 2021 and 2026 to strengthen coding and information and communication technology skills. Financed through a loan from the Council of Europe Development Bank (CEB), the project focuses on improving the information and communication technology infrastructure of schools in Albania. The initiative combines investment in digital infrastructure with support for digital literacy (UNESCO, 2026). In Singapore, the "Guide to Positive Use" was developed in 2025 by the Ministry of Digital Development and Information, the Ministry of Education, the Ministry of Health, the Ministry of Social and Family Development, and the Centre for Evidence and Implementation. The guide provides practical, evidence-based recommendations to help young people and families make the best use of digital technologies while avoiding potential harms (Liu & Tan, 2025).

In the United Arab Emirates, the "AI for Safer Children Initiative" was launched in 2025 through international cooperation between the United Arab Emirates Ministry of Interior (MoI UAE) and the United Nations Interregional Crime and Justice Research Institute (UNICRI). The initiative aims to bring together global expertise, policy innovation, and advanced AI technologies to develop practical, scalable solutions that harness their potential to strengthen child-protection mechanisms worldwide (Ministry of Interior of the United Arab Emirates, 2025).

In Kazakhstan, the program "Protecting Children in Kazakhstan from Online Violence, Abuse and Exploitation," supported by the Safe Online Fund and planned for implementation between 2024 and 2026, aims to establish robust mechanisms to protect children from online risks in digital environments. Its principal objectives are as follows:

- Strengthening national legislation and preventive systems for combating online threats,
- Expanding the role of the information technology sector in protecting children,
- Providing children, parents, and teachers with education on the fundamentals of cyber safety,
- Improving services provided to children affected by online violence and digital abuse (UNICEF Kazakhstan, 2025).

3.5.4. Complaint, Reporting and Victim-Support Mechanisms

Dedicated reporting centers and helplines can provide accessible channels for reporting illegal content, cybercrime, and other forms of online harm, while also connecting victims and families with appropriate support. These mechanisms may address issues such as cyberbullying, children's online safety, illegal gambling, fraud, and privacy violations. One example is Türkiye's Internet Hotline (https://ihbarweb.org.tr/), established by the Information Technologies and Communication Authority (BTK) in 2007. The Hotline receives and assesses reports concerning online content related to offenses specified under the Law on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications. Websites, newsgroups, chat rooms, file-sharing platforms, and email accounts containing material related to matters such as encouragement of suicide, sexual abuse of children, obscenity, illegal gambling, and disinformation may be reported through the site (Internet Hotline, 2026). Individual complaints concerning violations of privacy in online publications may also be submitted through the center pursuant to the same Law. Hotlines operating within the Safer Internet Centres across the EU likewise receive and assess reports of illegal online content, particularly child sexual abuse material and hate speech (Bayzan, n.d.).

Other countries have developed mechanisms that combine reporting with advice, referral, or victim support. The Digital Wellbeing Support Line was launched by the United Arab Emirates Digital Wellbeing Council to support families and parents in protecting children and young people in digital environments and improving the quality of their digital lives. Through this line, specialists provide families with professional advice on internet safety, cyberbullying, and harmful online content (WAM, 2020). In Bahrain, the Cybercrime Reporting Hotline (992) is used to report online crimes. Citizens can also report digital evidence, fake websites, and fraudulent messages through the official WhatsApp reporting line. Egypt's National Child Helpline 16000, operating under the National Council for Childhood and Motherhood (NCCM), the national mechanism for child rights and protection, provides 24/7 multi-channel support via telephone, WhatsApp, and web chat. The helpline receives reports of online harms such as cyberbullying, blackmail, and threats and refers them to the relevant authorities (Better Internet for Kids, 2026). In Morocco, the Espace Maroc Cyberconfiance Helpline, managed by the Moroccan Center for Polytechnic Research and Innovation (CMRPI), provides 24/7 support via email, WhatsApp, SMS, and telephone. The helpline receives and processes reports of violent, inappropriate, or illegal content published on social media platforms and provides victims with legal advice and psychological support.

3.6. Patterns, Gaps, and Emerging Policy Challenges in the OIC Member Countries

OIC Member Countries have different levels of digital maturity due to their economic, geographic, and social characteristics. According to the World Bank's GovTech Maturity Index (GTMI) 2025, which monitors public-sector digital transformation worldwide, slightly more than half of the OIC Member Countries covered fall within the two higher maturity groups, while slightly less than half fall within the two lower groups (Table 3.2). As shown in the table, 28.6% of OIC Member Countries are in the "Extensive GovTech Maturity Group" for public-sector digital transformation. Considering all countries included in the study, OIC Member Countries account for 20% of the 80 countries in this group. In the second category, the "Significant GovTech Maturity Group," 23.2% of OIC Member Countries are represented. Considering all countries, OIC Member Countries account for 31% of the 42 countries in this group. In the third category, the "Medium GovTech Maturity Group," 25% of OIC Member Countries are represented. Across all countries, OIC Member Countries account for 29.8% of the 47 countries in this group. In the fourth category, the "Low GovTech Maturity Group," 23.2% of OIC Member Countries are represented. OIC Member Countries account for 46.4% of the 28 countries in this group, which are considered to lag in digital transformation.

Table 3.2 OIC Member Countries by GTMI Groups, 2025

GTMI Group	Number of Countries	Number of OIC Member Countries	OIC Member Countries
A - Extensive GovTech Maturity	80 (41%)	16 (28.6%)	Albania, Azerbaijan, Bahrain, Bangladesh, Egypt, Indonesia, Jordan, Kazakhstan, Malaysia, Oman, Qatar, Saudi Arabia, Türkiye, Uganda, United Arab Emirates, Uzbekistan
B - Significant GovTech Maturity	42 (21%)	13 (23.2%)	Algeria, Benin, Brunei Darussalam, Côte d'Ivoire, Guinea, Iran, Kuwait, Kyrgyz Republic, Morocco, Nigeria, Pakistan, Togo, Tunisia
C - Medium GovTech Maturity	47 (24%)	14 (25%)	Burkina Faso, Cameroon, Gabon, Guyana, Iraq, Lebanon, Maldives, Mali, Mauritania, Mozambique, Senegal, Sierra Leone, Suriname, Tajikistan
D - Low GovTech Maturity	28 (14%)	13 (23.2%)	Afghanistan, Chad, Comoros, Djibouti, Gambia, Guinea-Bissau, Libya, Niger, Somalia, Sudan, Syrian Arab Republic, Turkmenistan, Yemen
Total	197	56	

Source: World Bank GovTech Maturity Index 2025 (Palestine is not included).

This distribution demonstrates that OIC Member Countries do not share a single digital-maturity profile, making uniform policy packages inappropriate. Lower-capacity settings may need to prioritize infrastructure, basic digital skills, institutional coordination, and accessible protection channels, whereas higher-capacity settings may be able to place greater emphasis on algorithmic transparency, platform accountability, privacy- and safety-by-design, and independent oversight. The common analytical baseline is functional rather than technological: families need meaningful access, trustworthy systems, prevention, and effective remedy regardless of the maturity level at which those functions are delivered.

Challenges related to infrastructure, the quality and reliability of internet access, the modernization of telecommunications systems, and continued reliance on paper-based processes can affect the pace and effectiveness of digital transformation and e-government initiatives. Resource constraints, varying levels of human and technical capacity, evolving legal and regulatory frameworks, institutional coordination challenges, varying levels of public awareness, and differences in the adoption of new technologies may also affect the pace of the digital transformation process. The digital divide among OIC Member Countries, arising from economic, social, motivational, and infrastructural factors, may delay the implementation of policies designed to protect children and families from risks in digital environments.

Although OIC Member Countries differ in the maturity of public-sector digital transformation, there are examples of digital family and child governance practices that align with cultural values. Examples from Türkiye include safe-internet initiatives (Safe Internet Service, Internet Help Center, Safe Web, Safe Gaming, Safe Child, and Safe Internet Center), as well as the "Guide to Protection from Cybercrime and Cyberbullying" and the "Parent Guide to Protecting Children from Digital Risks," published in 2025 by the Ministry of Family and Social Services of the Republic of Türkiye. Other examples include the use of AI technologies in child-protection systems established in the United Arab Emirates to ensure children's online safety (Ministry of Interior of the United Arab Emirates, 2025) and the establishment of the Digital Quality of Life Council to make decisions aimed at protecting moral, social, and cultural values consistent with Islamic teachings.

Across different national contexts, areas that may require further policy attention include the following:

- Scope for further development of dedicated legal frameworks aimed at protecting children and families online,
- Further integration of family-centered approaches into digital policies, which often focus on economic growth or infrastructure,

- Digital communication gaps between parents and children, and the need for effective standards of legal protection,
- The need to further strengthen informed digital awareness among parents within a framework of ethical and moral values
- Differences among OIC Member Countries in levels of institutional digital maturity,
- Varying capacities to respond to rapidly evolving technological change,
- Challenges in ensuring that global technology companies respond effectively to national legal and regulatory requirements.

These challenges do not arise solely from differences in technical capacity. Responsibilities for children's online protection, education, social services, data protection, cybersecurity, telecommunications, and the digital economy are distributed across different institutions, where shared objectives, referral protocols, and accountability mechanisms may vary in their level of development. This distribution can result in institutional fragmentation. Such fragmentation can make it more difficult for families encountering digital risks to access prevention, reporting, support, and remedy services in an integrated manner.

An important consideration from an inclusion perspective is the gap between the availability of digital services and the capacity to use those services safely and effectively. Family members who live in rural areas, have low incomes, are older, have disabilities, or have limited digital skills may not benefit equally from online services due to differences in device quality, connectivity costs, accessibility, language, and reliable support channels. Digital inclusion should therefore be assessed not only through internet access, but also through indicators of meaningful use, digital skills, accessible design, and reliable institutional support.

Another area for policy attention is the integration of national digitalization strategies and family-centered governance. Strategies often emphasize infrastructure, economic modernization, e-government, and innovation while children's online safety, parental guidance, intergenerational communication, family privacy, information integrity, and value transmission may receive comparatively less attention. Integrating a family-and-child impact lens into major digital policies provides a concrete way to operationalize the Section 1 framework without inserting Islamic terminology into every technical instrument.

The differences in GovTech maturity shown in Table 3.2 demonstrate that applying the same pace, tools, and institutional model across all OIC Member Countries is unlikely to be appropriate. In countries with low and medium levels of maturity, basic infrastructure, digital skills, institutional coordination, and accessible channels for redress may require greater emphasis; in countries with higher levels of maturity, algorithmic transparency, platform accountability, privacy- and safety-oriented design, independent oversight, and family-centered service integration can be strengthened. In this way, shared values and protection objectives can be maintained while implementation instruments are differentiated according to national capacity and socio-cultural context.

4. SELECTED COUNTRY CASE STUDIES: POLICY APPROACHES AND GOOD PRACTICES IN DIGITAL FAMILY GOVERNANCE

The case studies apply the analytical framework developed in Sections 1–3 rather than presenting independent country descriptions. Each case follows a common structure covering the country context, regulatory framework, institutional governance structure, implementation mechanisms and policy instruments, and lessons learned. The Core Islamic Principles are applied selectively at relevant points in the analysis to provide a value-based perspective on policies, practices, and their implications for families and children.

The comparative case analysis is based primarily on desk research drawing on official strategies, legislation, institutional documents, international datasets, program materials, and relevant academic literature. Where available, structured questionnaire responses and stakeholder inputs were used to complement the documentary analysis and provide additional context on implementation arrangements. Given differences in the availability and scope of country-level evidence, these additional inputs were used to inform the individual case studies rather than as a uniform source of comparative evidence across all countries.

The case studies cover four OIC Member Countries—Türkiye, Malaysia, Jordan, and Nigeria—reflecting different regional and policy contexts relevant to digital family governance. Hungary is included as a non-OIC reference case, providing an additional perspective from the EU digital regulatory environment. The selected countries differ in their demographic and socioeconomic characteristics, as well as in their approaches to digitalization, family and child policies, and related institutional arrangements. These differences provide a basis for examining a range of policy approaches and practices and considering their relevance to different OIC contexts.

4.1. TÜRKİYE

4.1.1. Introduction

Although Türkiye's population remains relatively young, the rising median age and growing share of the elderly population point to an ongoing process of demographic ageing. High levels of urbanization, together with expanding digitalization, provide an important socio-demographic context for examining both the opportunities and challenges that media and digital environments present for family life and relationships. According to data from the Turkish Statistical Institute (TurkStat), more than 93% of the population resides in urban settlements, while the median age has been rising steadily. Alongside these trends, the internet usage rate increased from 41.6% to 90.9% between 2010 and 2025 (TurkStat, 2025; Information and Communication Technologies Authority [ICTA], 2026). These demographic and digital trends provide an important backdrop for understanding changes in everyday family life and the contexts in which family relationships and practices are evolving. In Türkiye, this changing context is contributing to a social fabric in which established family and social values increasingly interact with modern and digital practices.

Intersection of Urbanization, Population Structure and Digitalization

Türkiye's high level of urbanization, together with changes in population and household structure, provides an important context for understanding the changing conditions of family life. Patterns of fertility, household size, population ageing, and the age of mothers at first birth indicate significant demographic change over time, as summarized in Table 4.1 (TurkStat, 2026). In this increasingly urban context, family life is also evolving from settings traditionally characterized by stronger extended-family and neighborhood networks toward living arrangements in which physical neighbourly interaction may be more limited, particularly with the widespread prevalence of apartment living. These developments are occurring alongside the rapid expansion of digital connectivity, creating a context in which established forms of family and neighborhood interaction increasingly coexist with digital communication and participation.

Digitalization can affect family relationships in different ways. While it may reduce some forms of face-to-face interaction, digital communication tools can also help sustain relationships when family members and social networks are physically dispersed. Video calls, messaging applications, including family groups, and social media provide additional channels through which family, kinship, and neighborhood ties can be maintained across geographical distance.

According to electronic communications sector market data published by the Information and Communication Technologies Authority (ICTA), the number of mobile broadband subscribers increased from 51.7 million in 2016 to 78.3 million in 2025 (ICTA, 2026). This expansion indicates the growing availability of the technical infrastructure that enables families to access and use digital services.

Table 4.1 Key Indicators on Family and Population Transformation

Total Fertility Rate 2005: 2,12 → 2025: 1,42	Age of Mother at First Birth 2005: 27 → 2025: 29,4	Child Population (0–17) 2007: %31,6 → 2025: %24,8
Household Size 2008: 4,00 → 2025: 3,08	Median Age 2007: 28,3 → 2025: 34,9	Elderly Population (65+) 2007: %7,1 → 2025: %11,1

Source: Data from Turkish Statistical Institute (TurkStat, 2026).

Transformation in Intra-Family Communication Dynamics

The increase in internet use from 13.9% in 2004 to 90.9% in 2025 shows how deeply digital technologies have become embedded in everyday life, creating an important context for changes in intra-family communication. In traditional family life in Türkiye, face-to-face interactions, including shared meals, family and neighbour visits, and conversation, have played an important role in socialization and the transmission of values (Ministry of Family and Social Services, 2021). Today, smartphones and social media are increasingly present within these shared spaces and routines. The report uses the descriptive expression "alone together" to capture situations in which family members are physically present in the same space while their attention and interaction are increasingly mediated by individual digital devices.

This development is particularly relevant in the context of Türkiye's strong tradition of family conversation, social interaction, and sharing. Digital tools can enable family members to remain in frequent and immediate contact, including when they are physically apart—for example, allowing a working parent to communicate with a child during the day. At the same time, intensive individual device use during shared family time may reduce opportunities for face-to-face interaction and emotional exchange. This concern is reflected in the usage patterns presented below: 21.0% report using a smartphone while eating with others, while 25.5% report spending less time with their family because of screen time. These findings suggest that the issue is not simply the presence of digital technologies in family life, but how and when they are used within shared family routines.

Internet use has become widespread across age groups. As shown in Table 4.2, internet use among individuals aged 16–74 increased from 13.9% in 2004 to 90.9% in 2025, while the proportion of households with internet access rose from 19.7% in 2007 to 96.2% in 2025. Internet use in 2025 exceeds 90% among all age groups between 16 and 54, indicating that digital participation now extends across much of the adult population.

Table 4.2 Internet Use by Age Group

Age groups	2004 (%)	2025 (%)
16-24	%26,6	%97,8
25-34	%15,7	%98,1
35-44	%9,4	%97,3
45-54	%5,5	%92,4
55-64	%1,6	%78,4
65-74	%0,4	%53,2

Source: Turkish Statistical Institute (TurkStat, 2025/2026).

The rate of Internet use among individuals aged 16–74 rose from 13.9% in 2004 to 90.9% in 2025. Meanwhile, the proportion of households with Internet access increased from 19.7% in 2007 to 96.2% in 2025.

Data on digital practices provide further insight into how screen and device use intersect with everyday routines. TurkStat's *Survey on Information and Communication Technology (ICT) Usage in Children* (TurkStat, 2024) and the *Digital Türkiye* reports by We Are Social and Meltwater (2024, 2025) provide complementary evidence on patterns of digital and screen use. As shown in Table 4.3, the proportion reporting six or more hours of daily use is higher at weekends than on weekdays.

Table 4.3 Daily Screen Use of Six Hours or More

6+ Hours of Daily Use	Rate (%)
Weekdays	%7,0
Weekends	%10,3

Source: TurkStat (2024/2025)

Table 4.4 provides a broader picture of how digital use intersects with daily routines and social relationships. Frequent phone checking and smartphone use during shared activities coexist with reported effects on reading, studying, family time, face-to-face interaction, and sleep. Notably, 25.5% report spending less time with their family because of screen time. In addition, internet use is broadly similar among males and females (92.2% and 90.3%, respectively), while the difference is more pronounced in digital gaming, with rates of 82.8% among males and 64.8% among females.

Table 4.4. Selected Indicators of Digital Use, Daily Routines and Social Relationships

Indicator	Rate (%)
A. Digital-Use Behaviors	
Checking one's phone at least once every 30 minutes	32.6
Checking one's phone as the last activity before going to sleep	30.6
Checking one's phone immediately after waking up	22.7
Using a smartphone while watching TV	21.5
Using a smartphone while eating with others	21.0
B. Reported Effects of Screen Time	
I read fewer books	34.4
I study less	33.3
I spend less time with my family	25.5
I meet my friends face-to-face less often	18.6
I sleep less	17.2
C. Selected Indicators of Digital Use	
Internet use	91.3
Having a mobile phone for personal use	43.9
Social media use (top three platforms: YouTube, Instagram, TikTok)	66.1
Digital gaming	74.0

Source: TurkStat (2025), Survey on Information and Communication Technology (ICT) Usage in Children

Intergenerational Digital Divide and Authority Relations

The transformation in Türkiye's age structure—the declining share of the younger population and the growing share of the elderly—makes differences in digital competence more visible within families where three generations coexist.

While respect for elders has traditionally been an important feature of family relations in Türkiye, younger family members may possess greater knowledge and practical competence in the use of digital technologies. This can alter established patterns of knowledge exchange between generations without necessarily changing broader family authority relations.

"**Reverse socialization**" has been used in the family sociology literature to describe the process through which younger generations transfer their knowledge of new technologies to older generations, thereby reversing the traditional direction of knowledge transfer from older to younger generations (Singh, 2021).

Grandparents seeking assistance from their grandchildren in using digital devices provide a practical example of this changing direction of intra-family knowledge transfer and the dynamic described as "reverse socialization" (Singh, 2021).

This situation may also create new challenges for parents' traditional role in supervising and guiding their children. Findings from the Türkiye Family Structure Survey (TAYA) indicate that adolescents, in particular, can establish social networks beyond direct parental oversight through social media, gaming platforms, and messaging applications. Compared with interactions in the physical neighborhood environment, parents may find it more difficult to observe whom their children communicate with in digital environments or the types of content to which they are exposed. This changing context may create new concerns for families and increase the need for appropriate forms of parental guidance and digital safety.

Marriage, Couple Relationships and Social Media

High rates of internet and social media use affect not only parent–child relations but also relationships between spouses. Images of the "ideal family" and "happy marriage" shared on social media platforms may create comparison-based pressures among young couples and may influence marital satisfaction and expectations. The use of digital communication records, such as message histories and social media interactions, as evidence in divorce cases also illustrates the growing importance of digital traces in matters of trust, privacy, and legal assessment within marital relationships.

Accordingly, an important effect of digitalization on family life can be observed at the relational level, beyond individual patterns of screen use. Since individuals sharing the same household may direct their attention to different screens even while physically together, shared time can become a simultaneous yet disconnected experience. Research also suggests that the presence of a mobile device can affect the quality of face-to-face interaction. The phenomenon of "technoference," used to describe interruptions in interpersonal interactions caused by attention to digital devices, including during parent–child interactions, illustrates how digital-device use can interfere with moments of interpersonal connection (McDaniel & Radesky, 2018).
Furthermore, in terms of reconciling work and family life, the constant accessibility enabled by mobile communication technologies can blur the boundaries between work and family. Work-related communication outside regular working hours may interfere with shared family time and contribute to work–family conflict. This issue is particularly relevant for dual-career families, for whom the boundaries between professional and family responsibilities may be especially difficult to manage (Tunç et al., 2020).

Opportunities and Risks of Digitalization for Family Life

Assessing the impact of digitalization on family relations solely through its risks would provide an incomplete picture. Türkiye's high level of internet use and extensive mobile connectivity provide families with new opportunities for communication, access to information, education, and mutual support (Information and Communication Technologies Authority [BTK], 2025). These opportunities include:

- maintaining regular communication through video calls with family members living abroad or in other cities;
- facilitating rapid information-sharing and solidarity during family crises, including illness and disasters such as earthquakes;
- enabling parents to access and exchange knowledge and experience through online parenting forums and groups;
- allowing families to become more involved in children's educational processes through distance education and digital literacy initiatives; and

- supporting family businesses and women's entrepreneurship through digital platforms (Presidency of the Republic of Türkiye Digital Transformation Office, 2021–2025).

At the same time, the widespread use of digital technologies can introduce new socio-cultural risks and challenges into family life. Changes in communication patterns, children's increasing engagement with digital environments, and differences in digital competence between generations may require families to adapt established practices of guidance, supervision, and interaction. In this context, strengthening digital literacy and media awareness within families remains important.

These changes are also taking place alongside broader transformations in Türkiye's social environment. As discussed earlier, changing patterns of neighborhood interaction, particularly in metropolitan settings, may affect some of the informal forms of social interaction and support that have traditionally surrounded family and community life. Parents may therefore rely increasingly on family-level strategies to guide and protect children's digital engagement. Research on digital parenting in Türkiye similarly highlights the growing importance of parents' capacity to assume appropriate digital parenting roles (Manap & Durmuş, 2021).

These developments illustrate the dual character of digitalization for family life. Digital environments can help families maintain relationships across distance, access knowledge and services, support children's education, and create new economic opportunities, while also requiring families to develop new capacities for guidance, communication, and protection. The policy challenge is therefore not simply to expand or restrict digital participation, but to enable families to benefit from digital opportunities while strengthening their capacity to respond to associated risks.

Evaluation: Türkiye's Family Structure Between Transformation and Adaptation

When TurkStat's demographic and socio-economic data are considered together with Türkiye's digital transformation indicators, the transformation appears neither wholly negative nor wholly positive. Family life in Türkiye continues to be shaped by traditional elements such as neighbourhood culture, neighbourly relations, and social solidarity, while also adapting to new forms of communication and socialization associated with widespread internet use and mobile technologies. As patterns of physical neighbourhood interaction change, digital tools can also enable family members to maintain communication across distance, while differences in digital competence between generations contribute to new forms of mutual learning.
While high-level policy frameworks such as the National Artificial Intelligence Strategy (2021–2025) and the Digital Türkiye initiative support Türkiye's broader digital transformation, stronger integration of family-based digital literacy, media education, and parental support programmes into these frameworks could further strengthen a family-centred approach.

Overall, media and digital environments in Türkiye are not eliminating family relationships but are reshaping the ways in which family members communicate and interact. Supporting families through this transformation requires not only investment in technological infrastructure but also a strong family-based approach to media and digital literacy and continued support for parents and caregivers.

Value-Based Perspective

The findings of the Türkiye case can also be considered through the report's value-based framework. The role of digital technologies in helping family members maintain communication and relationships across distance can be considered in relation to Hifz al-Usra, with its emphasis on the protection and well-being of the family. At the same time, findings concerning intensive device use during shared family time, including "alone together" experiences and technoference, highlight the relevance of Wasatiyyah in balancing the opportunities offered by digital technologies with their potential effects on family interaction. Viewed together, these principles help assess how digital transformation affects family relationships and how its opportunities and risks can be balanced in ways that support family well-being.

4.1.2. Policy and Regulatory Framework

The family is a fundamental social institution through which love, respect, cultural values, and traditions are transmitted across generations. It also plays an important role in passing national and cultural values on to younger generations. As a primary source of security, belonging, and support for individuals, the family can also serve as a "safe haven."

In recent years, rapid technological developments have brought significant changes across many areas of social life, and family life has also been affected by the dynamics of digital transformation. In this context, protecting children and young people from harmful content and influences that may undermine their well-being, family relationships, and societal values is regarded as a shared responsibility across society.

Accordingly, the Vision Document and Action Plan for the Protection and Strengthening of the Family (2024–2028) was prepared to strengthen the family institution, reinforce intergenerational bonds, and enhance social solidarity. In this context, 2025 was declared the "Year of the Family," accompanied by a range of initiatives. With a view to developing family policies within a long-term, holistic, and sustainable framework, the period 2026–2035 has also been designated the "Decade of Family and Population."

During this ten-year period, guided by the principle of "Strong Individual, Strong Family, Strong Society," the emphasis is on protecting and strengthening the family institution and supporting its continuity across generations. Within the broader "Century of Türkiye" vision, strong families are regarded as an important foundation for social stability and well-being.

The policy and legislative framework seek both to protect families from digital risks and to support family members in engaging with the digital environment in an informed, responsible, and productive manner. This section addresses:

- national strategies, policy documents, and legislation, including the legal mandates and responsibilities of relevant institutions;
- regulatory instruments concerning digital platforms and content;
- the legal framework for oversight, enforcement, reporting mechanisms, and relevant reporting platforms;
- the place of preventive policies, including education, awareness-raising, guidance, and information, within the regulatory and policy framework; and
- practical tools for digital safety and parental guidance, including parental control and related mechanisms.

4.1.2.1. National Strategy, Policy Documents, and Legislation: Legal Definitions and Scope of Duties of Responsible Institutions

Türkiye seeks both to protect families from digital risks, including problematic technology use, cyberbullying, and exploitation, through legislation and regulatory mechanisms, and to strengthen the capacity of families to engage with the digital environment safely and responsibly through education and awareness-raising policies. The key policy documents addressed in this section are summarized below.

Table 4.5 Key National Policy Documents Relevant to Digital Family Governance

Policy Document	Period	Target Group	Relevance to Digital Family Governance
Vision Document and Action Plan for the Protection and Strengthening of the Family	2024–2028	Families	Addresses the implications of digitalization for family life and promotes family-friendly approaches
Türkiye Child Rights Strategy Document	2023–2028	Children	Addresses the protection and exercise of children's rights in digital environments
Action Plan for Combating Behavioral Addictions	2024–2028	Children, youth, and families	Addresses risks associated with technology, internet, and screen use
Action Plan for the Empowerment of Children in the Digital World	2026–2030	Children, parents, and relevant professionals	Addresses digital risks through awareness-raising, intervention, and institutional coordination

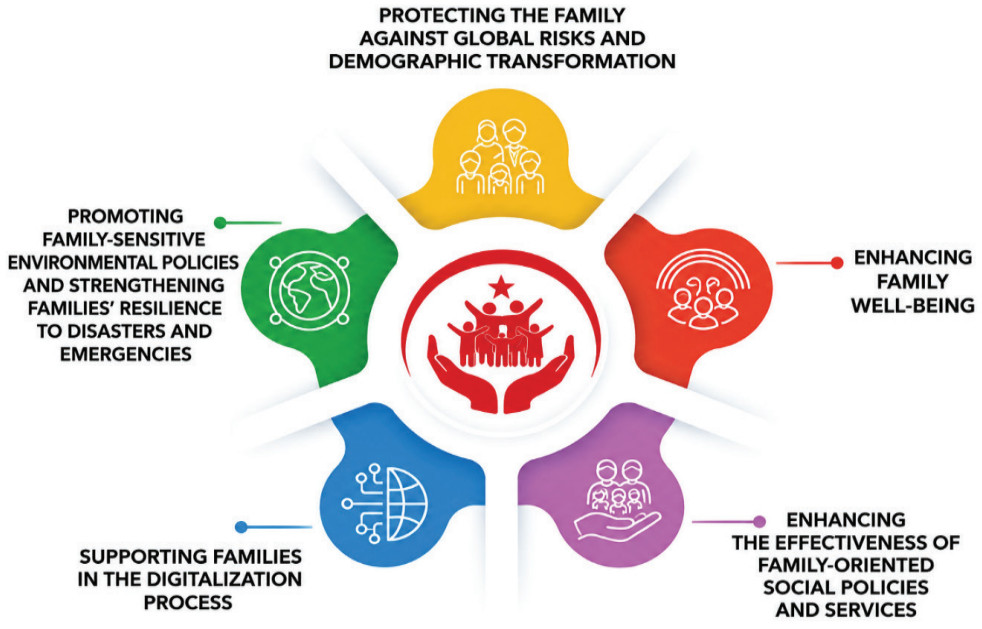
Source: Created by the Authors

Vision Document and Action Plan for the Protection and Strengthening of the Family (2024-2028)
Developing and implementing family-oriented policies and initiatives through a participatory approach involving all relevant stakeholders is important for enhancing the quality, reach, and effectiveness of services for families. Prepared under the auspices of the Presidency of the Republic of Türkiye and coordinated by the Ministry of Family and Social Services, the *Vision Document and Action Plan for the Protection and Strengthening of the Family (2024–2028)* brings together the efforts of public institutions and organizations, local authorities, universities, civil society organizations, and other relevant stakeholders to strengthen the family, the institution of marriage, and family members.

As the first national policy document with this specific focus, it aims to enhance the effectiveness of policies and services for the protection and strengthening of the family through cooperation and coordination among relevant stakeholders (Ministry of Family and Social Services, 2024).

The Vision Document and Action Plan is structured around five core strategic objectives aimed at developing effective social policies and practices in the areas of population, education, culture, technology, and media, while addressing education, working life, and social life, as presented in Figure 4.1.

Figure 4.1 Scope of the Vision Document and Action Plan for the Protection and Strengthening of the Family



Source: Prepared by Authors based on Vision Document and Action Plan for the Protection and Strengthening of the Family

Among these thematic areas, "Supporting the Family in the Process of Digitalization" was formulated in recognition of the significant role of traditional and new media in shaping families' values and attitudes. Rapid changes and developments in information and communication technologies have significant implications for the family institution. Harmful trends and practices increasingly circulating through media at the global level may adversely affect family members, particularly children and young people, and may weaken intra-family communication.

As the proportion of households with internet access increases, children's internet use patterns and the risks to which they may be exposed are becoming increasingly important. Risks of behavioral addiction associated with social media use have also emerged as a growing concern, with potential adverse effects on family members, particularly children, including their psychological well-being and cognitive and social development. Research findings highlight the importance of a family-sensitive approach to media communication and broadcasting, comprehensive research on the effects of internet use on families, and raising awareness among all family members—particularly parents—of digital risks and safe-use practices.

Addressing the adverse effects associated with social media use, digitalization, and technological developments requires coordination among relevant institutions as well as cooperation with the media sector. In this context, supporting families in adapting to technological developments while protecting family structure, intra-family relationships, and family values from the risks associated with digitalization has become increasingly important.

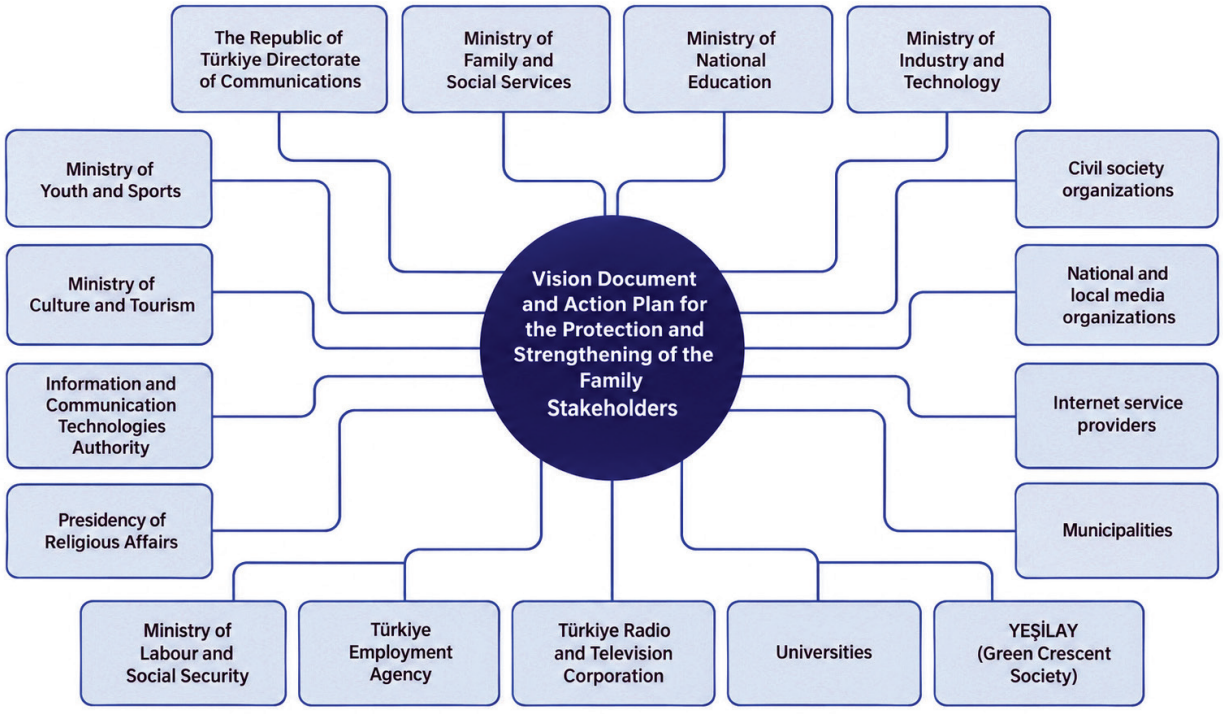
Accordingly, under "Supporting the Family in the Process of Digitalization," the following objectives have been identified:

- Promoting the informed use of media and technology and reducing digital addictions;
- Increasing family-friendly media productions and digital content, as well as access to such content; and
- Protecting the family and family values in media and digital environments.

The main stakeholders of the Vision Document and Action Plan for the Protection and Strengthening of the Family, as presented in Figure 4.2, include:

- Public institutions and local authorities;
- Academic institutions and experts;
- Civil society organizations and professional associations;
- Media and broadcasting organizations; and
- Families and individuals.

Figure 4.2 Stakeholders of the Vision Document and Action Plan for the Protection and Strengthening of the Family



Source: Created by the Authors

Target groups of the Vision Document and Action Plan for the Protection and Strengthening of the Family include:

- Public institutions and local authorities;
- Academic institutions and experts;
- Civil society organizations and professional associations;
- Media and broadcasting organizations; and
- Families and individuals.

The responsible institutions and the activities to be undertaken under the three strategic objectives related to supporting the family in the digitalization process are summarized in Table 4.6.

Table 4.6 Responsible Institutions and Selected Activities for Supporting the Family in the Process of Digitalization

Strategic Objective	Responsible Institution	Activities
Strategic Objective 10: Promoting the Conscious Use of Media and Technology and Reducing Digital Addictions	Information and Communication Technologies Authority (BTK)	• Development of brochures, guides, animations, and public service announcements on safe internet use and the conscious use of technology and social media. • Promotional activities to increase the number of Safe Internet Service (GİH) subscribers.
	Ministry of Family and Social Services	• Expansion of training activities on media literacy, digital parenting, cyberbullying, and digital crimes. • Family education and workshops aimed at strengthening intergenerational communication.
	Ministry of National Education	• Wider implementation of digital literacy education programmes in schools.
	Ministry of Youth and Sports	• Expansion of training, seminars, and camps to promote the conscious use of technology and media among young people. • Organization of sports and cultural activities as part of efforts to combat digital addiction.
	Ministry of Industry and Technology	• Development of lifelong learning programmes to facilitate older adults' access to digital services.
	Ministry of Culture and Tourism	• Organization of artistic and cultural activities aimed at increasing the time families spend together.
Strategic Objective 11: Increasing Family-Friendly Media Productions and Digital Content and Expanding Access to Them	Turkish Radio and Television Corporation (TRT)	• Ensuring that new productions developed through traditional and new media are protective, guiding, and family-friendly.
	Radio and Television Supreme Council (RTÜK)	• Expansion of support for efforts to promote family- and child-friendly productions and series.
	Ministry of National Education	• Development of protective, guiding, and family-friendly media productions and digital content within the Education Informatics Network (EBA) to increase families' access.
	Ministry of Culture and Tourism	• Provision of mobile cinema activities in settlements with limited access to such services.
	Ministry of Family and Social Services	• Development of an educational, developmental, and guidance-oriented mobile application on family life skills and parenting.
Strategic Objective 12: Protecting the Family and Family Values in Media and Digital Channels	Ministry of Family and Social Services	• Expansion of family-themed broadcasts and programmes within the scope of family education programmes across national and local media. • Organization of local "Family and Media" meetings with institutions, organizations, and universities working in the fields of family and media.
	Radio and Television Supreme Council (RTÜK)	• Priority broadcasting, in the same time slot, of public-interest programmes on media literacy and the conscious use of technology in place of programmes suspended as a result of administrative measures.
	Ministry of Industry and Technology	• Development and dissemination of technology programmes for families on the conscious and effective use of technology.

Source: Ministry of Family and Social Services (2024), Vision Document and Action Plan for the Protection and Strengthening of the Family (2024–2028).

These strategic objectives seek to strengthen families' capacity for conscious, safe, and balanced engagement with digital technologies, including parents' ability to guide children's digital media use in accordance with their age and developmental needs. They also emphasize protecting children and young people from digital addiction and harmful content, expanding access to family-friendly and quality digital content, and promoting the constructive use of digital media to support family communication and intergenerational interaction. Overall, the framework combines protection from digital risks with efforts to enable families to benefit from the opportunities of digital transformation.

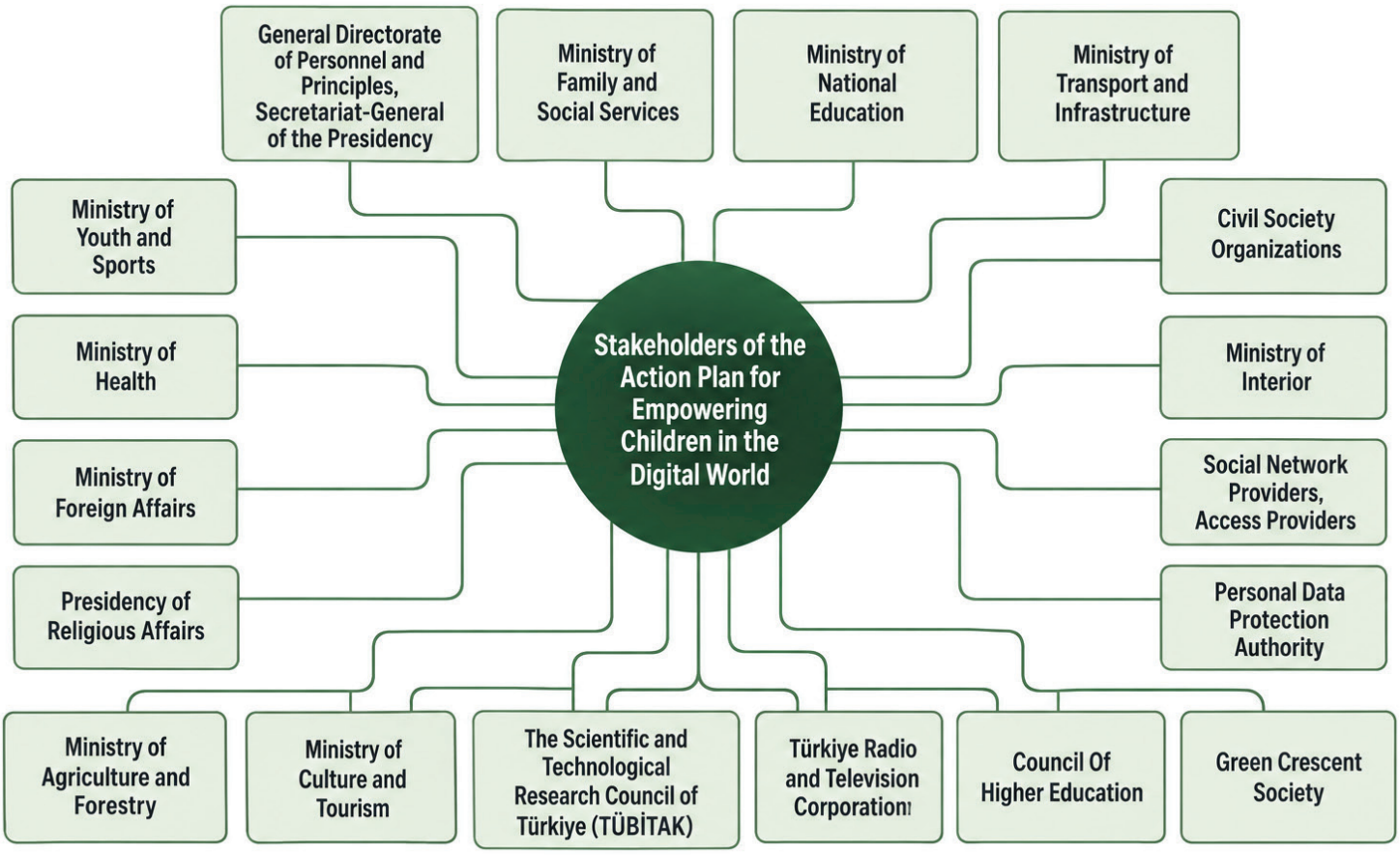
Implementation of the Action Plan is supported by a monitoring and evaluation mechanism coordinated by the General Directorate of Family and Community Services of the Ministry of Family and Social Services. Responsible institutions report annually on implementation in cooperation with relevant stakeholders, and the Ministry consolidates these inputs into Monitoring and Evaluation Reports. A General Analysis and Evaluation Report is also envisaged one year before the end of the implementation period to assess progress and inform the preparation of the subsequent action plan.

Action Plan for the Empowerment of Children in the Digital World (2026-2030)

Children may face particular challenges in recognizing and responding to risks in the complex and rapidly evolving digital environment. For this reason, a holistic approach grounded in the best interests of the child is needed, addressing both protection from risks and safe access to the opportunities offered by digital technologies. This approach encompasses not only children's individual development but also their participation in the digital environment as informed, responsible, and rights-aware individuals. The dynamic and constantly evolving nature of the digital environment also requires efforts to protect and empower children to be pursued through innovative, flexible, and multi-stakeholder approaches. Accordingly, the Action Plan for the Empowerment of Children in the Digital World (2026–2030), prepared under the leadership of the Ministry of Family and Social Services, provides a strategic framework for adapting Türkiye's child protection policies to the requirements of the digital age.

The Action Plan aims to protect children from risks they may encounter in digital environments, promote equal, safe, and informed access to digital opportunities, and foster a child protection culture involving society as a whole. To this end, it provides for national-level coordination of policies concerning children in the digital environment, systematic mechanisms for risk prevention, stronger digital awareness among children, families, and professionals, and the development of child-friendly digital technologies.

Figure 4.3 Stakeholders of the Action Plan for Empowering Children in the Digital World



Source: Prepared by the Authors based on the Action Plan for Empowering Children in the Digital World.

The Action Plan is structured around four core strategic objectives aimed at ensuring children's safety in the digital world and enabling them to make the best use of digital opportunities, as presented in Figure 4.4.

Figure 4.4 Strategic Objectives of the Action Plan for the Empowerment of Children in the Digital World (2026–2030)



Source: Prepared by authors based on the Action Plan for the Empowerment of Children in the Digital World (2026–2030)

The Action Plan for the Empowerment of Children in the Digital World (2026–2030) is implemented under the auspices of the Presidency of the Republic of Türkiye and coordinated by the Ministry of Family and Social Services. It aims to protect children from digital risks, enable them to make the best use of digital opportunities, and empower them as safe, informed, and productive individuals. The monitoring and evaluation process is coordinated by the General Directorate of Child Services of the Ministry of Family and Social Services.

Türkiye Child Rights Strategy Document and Action Plan (2023–2028)

Under the strategic objective of "Access to Information Technologies and Safe Internet Use," nine sub-activities support coordinated efforts to protect children from exploitation and other risks in digital environments. The responsible institutions and activities under the relevant strategic targets are summarized in Table 4.7.

Table 4.7 Strategic Targets, Responsible Institutions and Activities under "Access to Information Technologies and Safe Internet Use"

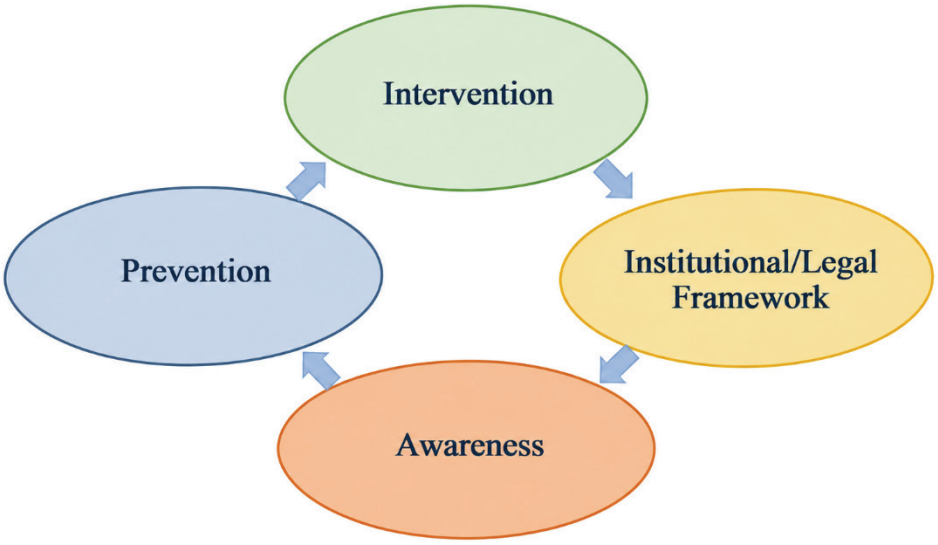
Strategic Target	Responsible Institution(s)	Activities
2.6.1. Protecting Children from the Risks of Digital Environments and Supporting Their Development	Information and Communication Technologies Authority (BTK)	Establishment of a control and coordination mechanism to protect children from harmful content in digital environments.
	Information and Communication Technologies Authority (BTK) and Personal Data Protection Board	Protection of children from risks in digital environments, safeguarding personal data, ensuring privacy, and raising awareness of children's digital rights.
	Radio and Television Supreme Council (RTÜK), Ministry of National Education, Ministry of Family and Social Services, and Ministry of Culture and Tourism	Development, dissemination, and promotion of child-friendly principles for visual, audio, and written media content.
	Information and Communication Technologies Authority (BTK) and Radio and Television Supreme Council (RTÜK)	Strengthening mechanisms to promote the dissemination of informational content developed for children on digital platforms and through mainstream media channels.
	Information and Communication Technologies Authority (BTK), Ministry of Industry and Technology, Ministry of Family and Social Services, and Ministry of National Education	Provision of training for children and parents to strengthen family communication and prevent digital addiction.
2.6.2. Taking Measures to Protect Children from Content That May Adversely Affect Their Development	Ministry of National Education	Revision of the education curriculum to address the opportunities and risks arising from emerging technologies; provision of education for children on internet ethics.
	Ministry of Family and Social Services, Ministry of National Education, and Ministry of Industry and Technology	Development of child-friendly applications, including websites and mobile applications, that can serve as alternatives for children, consider the needs of children with special needs, and include educational content.
	Ministry of Interior and Information and Communication Technologies Authority (BTK)	Awareness-raising activities on cyber fraud targeting children and adults.

Source: Türkiye Child Rights Strategy Document and Action Plan (2023–2028).

National Strategy Document and Action Plan for Combating Behavioral Addictions (2024–2028)
Action plan efforts initiated by the Ministry of Health in 2017 have continued under the coordination of the High Council for Combating Addiction. The National Strategy Document and Action Plan for Combating Behavioral Addictions was updated to cover the 2024–2028 period and aims to protect society from behavioral addictions related to technology, internet use, and gambling (Ministry of Health, 2024).

Regulation on the Procedures and Principles for Incentivizing Family- and Child-Friendly Productions and Series
Under the Regulation on the Procedures and Principles for Incentivizing Family- and Child-Friendly Productions and Series, dated 8 May 2018 and numbered 30415, the Ministry of Family and Social Services and the Radio and Television Supreme Council (RTÜK) jointly grant the Family- and Child-Friendly Production and Series Incentive Awards. The awards aim to encourage the broadcasting of family- and child-friendly productions and series that uphold the principle of protecting the family and children in broadcasting services and support family integrity and continuity, as well as the physical, mental, and moral development of children and young people (Regulation on the Procedures and Principles for Incentivizing Family- and Child-Friendly Productions and Series, 2018).

Figure 4.5 Digital Child Protection Policy Cycle



Source: Created by authors

The key legislative instruments relevant to digital family governance in Türkiye are summarized in Table 4.8

Table 4.8 Key Legislative Framework Relevant to Digital Family Governance in Türkiye

Legislative Instrument	Main Scope	Relevance to Digital Family Governance
Constitution of the Republic of Türkiye	Constitutional protection of the family, children, privacy, and fundamental rights	Provides the overarching legal basis for the protection of family life, children, privacy, and personal rights, including in digital environments.
Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication	Online content and the responsibilities of content, hosting, access, and social network providers	Provides key legal mechanisms for addressing unlawful online content and establishes responsibilities relevant to protecting children and families in digital environments.
Law No. 6698 on the Protection of Personal Data	Processing and protection of personal data, data-subject rights, and obligations of data controllers	Provides the principal legal framework for personal-data protection and privacy, with relevance to the protection of children's and families' personal data in digital environments.
Law No. 6112 on the Establishment of Radio and Television Enterprises and Their Media Services	Radio, television, and on-demand media services; broadcasting standards and protection of minors	Establishes safeguards concerning audiovisual media content, including provisions relevant to protecting children and young people from potentially harmful content.
Turkish Penal Code No. 5237	Criminal offences, including offences that may be committed or facilitated through digital means	Provides the criminal-law framework applicable to offences affecting children and family members that may also occur or be facilitated in digital environments.
Child Protection Law No. 5395	Protection of children in need of protection or involved in the justice system; protective and supportive measures	Provides the broader child-protection framework within which risks affecting children's safety and well-being, including those arising in digital environments, may be addressed.

Source: Compiled by the Authors based on relevant national legislation.

4.1.2.2. Regulatory Instruments for Digital Platforms and Content

Social Media Working Group

The Social Media Working Group was established within the Ministry of Family and Social Services to identify risks that children may encounter in digital environments, carry out protective and preventive activities in response to these risks, and develop measures to address emerging risks. The Working Group is coordinated by the General Directorate of Child Services. As part of its activities, content that children encounter or may encounter in digital environments is closely monitored, associated risks are identified, and preventive measures are undertaken. In this context, institutional and inter-institutional intervention processes are carried out in relation to content that may adversely affect children's development or in which children are or may be exposed to neglect or exploitation. Partner institutions in this process include the Information and Communication Technologies Authority (BTK), the Radio and Television Supreme Council (RTÜK), and the Department of Cybercrime of the General Directorate of Security.

In addition, where a child is identified as being at risk in the online environment, a Social Assessment Report is requested from the Provincial Directorate of Family and Social Services in the province where the case has arisen. Based on the findings of the report, an appropriate social service model is applied in accordance with the best interests of the child.

Regulation on the Presentation of Radio, Television and Broadcasts over the Internet
Law No. 6112 on the Establishment of Radio and Television Enterprises and Their Media Services entered into force upon its publication in the Official Gazette on 3 March 2011. The Law regulates radio, television, and on-demand broadcasting services in Türkiye and defines the duties and powers of the Radio and Television Supreme Council (RTÜK). The broadcasting service principles set out in Article 8 of the Law constitute the fundamental criteria for oversight. These include respect for human dignity, privacy, and personal rights in broadcasting services; protection of the physical, mental, and moral development of children; non-promotion of violence, discrimination, and hate speech; non-encouragement of addictive substances and harmful habits; and protection of the national and spiritual values of the family and society (Law No. 6112, 2011).

Sanctions applicable in cases of non-compliance are regulated under Law No. 6112 according to the nature of the violation and the type of broadcasting service concerned. Under Article 32, sanctions may include warnings, administrative fines, suspension of programmes, removal from the catalogue, temporary suspension of broadcasting, and revocation of broadcasting licences (Law No. 6112, 2011).

RTÜK is responsible for regulating and supervising broadcasting services, monitoring broadcasters' compliance with legislation, developing regulatory and preventive policies for the protection of children and young people, promoting media literacy, and conducting research and awareness-raising activities concerning risks in the broadcasting sector.

Under Article 21 of the *Regulation on the Provision of Radio, Television and On-Demand Broadcasting Services via the Internet*, organizations holding an internet broadcasting licence or broadcast transmission authorization are required to take measures to ensure parental control. Parental control refers to restricting or preventing children and young people's access through media devices to content that is inappropriate for their age or may be harmful to them (Regulation on the Provision of Radio, Television and On-Demand Broadcasting Services via the Internet, 2019).

4.1.2.3. Legal Framework of Oversight and Enforcement Mechanisms, Reporting Platforms, and Websites

Children Are Safe Website and Mobile Application
The Children Are Safe website and mobile application have been launched to support children in becoming aware of the risks they may encounter in digital environments and developing safe digital use skills; to provide guidance to parents and caregivers; to enable children, parents, and professionals working with children to report situations involving neglect, abuse, peer bullying, violence, and harmful digital content; and to facilitate access to appropriate support and referral mechanisms when needed.

The website and mobile application provide informative and guidance-oriented content on the risks that children, parents, and caregivers may encounter in digital environments. Through the "Ask for Help" section of the platform, children, parents, and citizens can submit reports concerning neglect, abuse, peer bullying, violence, and similar risks by attaching text, images, audio recordings, and location information. The platform also enables users to report content, broadcasts, and applications considered harmful to children. Depending on the nature of the submission, reports are referred to Ministry specialists or to the ALO 183 and ALO 112 hotlines, where necessary assessment and intervention processes are initiated.

The Children Are Safe website can be accessed at cocuklarguvende.gov.tr, while the mobile application is available through the App Store and Google Play Store.

The "Children Are Safe project, implemented by the Ministry of Family and Social Services of the Republic of Türkiye, was awarded the title of "WSIS Prizes 2026 Champion" under the WSIS Prizes 2026, organized under the umbrella of the United Nations and coordinated by the International Telecommunication Union (ITU).

The project was among the top five projects receiving the highest number of votes in its category out of 1,596 projects, and was selected as the Champion Project in its category.

Presidential Circular on the Accessibility of Websites and Mobile Applications
To support the equal participation of persons with disabilities and older persons in the digital environment, the "Monitoring Commission for the Accessibility of Websites and Mobile Applications" was established under the chairmanship of the Minister of Family and Social Services. Websites and mobile applications of institutions, organizations, universities, and legal entities that have completed the review process and are determined to meet accessibility requirements are granted the right to use the "Accessibility Logo" for a period of two years by the Ministry of Family and Social Services (Ministry of Family and Social Services, 2025).

4.1.2.4. Educational, Guidance and Information Tools

4.1.2.4.1. Ministry of Family and Social Services

Türkiye Combating Addiction Training
Under the protocol signed between the Türkiye Green Crescent Society (Yeşilay) and the Ministry of Family and Social Services, the Türkiye Combating Addiction (TBM) Trainings aim to raise awareness of addiction among Ministry personnel, children over the age of 15 in institutional care, and the general public. The TBM Trainings include modules on substance, alcohol, tobacco, gambling, and technology addiction (Türkiye Green Crescent Society, 2026).

Family Education Programme
The Family Education Programme, an adult education programme developed by the Ministry of Family and Social Services, includes media-related modules titled "Understanding Media," "Comprehending Media," "Conscious Media Use," and "Family and the Internet" (Ministry of Family and Social Services, 2026).

In response to the diversification of family structures and needs, the Family Education Programme was updated through the development of a Modular Family Education Programme, with nationwide dissemination completed in 2025. The updated programme consists of structured sessions delivered in small, closed groups or seminar format and is designed to support changes in parents' attitudes and behaviors. It comprises a total of 12 sessions, including eight main modules and four supplementary modules. "Social Media, Digital Games and Information Technology Tools" is among the modules (Ministry of Family and Social Services, 2026).

Awareness Education Programme for Strengthening and Developing Children's Life Skills
In line with measures included in the 11th and 12th Development Plans to provide children—and, under the 12th Development Plan, their parents—with awareness training on neglect, abuse, and violence from early childhood and to strengthen children's life skills, inclusive and modular education programmes are being developed to support children's life skills.

As the first stage of this initiative, the Awareness Education Programme for Strengthening and Developing Children's Life Skills was developed for parents and caregivers of children aged 0–6, with the aim of protecting children from neglect, abuse, and violence, enhancing their well-being, and supporting their healthy development (Ministry of Family and Social Services, 2026).

The programme consists of eight modules focusing on the prevention of neglect and abuse: "Prevention of Neglect and Abuse – Basic Information for Parents," "Parenting," "Development," "Sensitive Care," "Positive Discipline," "Daily Routines," "Digital Parenting," and "Interactive Routines: Playing and Reading." The "Digital Parenting" module provides parents with information aimed at strengthening their capacity to protect children aged 0–6 from digital risks.

The programme began implementation in June 2025, initially with a focus on provinces affected by the earthquake, and continues to be expanded in 2026. Modules are also being developed for the 7–18 age group, targeting both children and parents: "Children in the Digital World" for children and "Digital Parenting" for parents (Ministry of Family and Social Services, 2026).

Digital Detox Activities
The year 2025 was declared the "Year of the Family" with the aim of emphasizing the importance of the family, preserving unity and solidarity within the family, and supporting families in addressing existing risks. As part of the Year of the Family, Digital Detox Activities were organized across all 81 provinces. These activities continue to be expanded nationwide in 2026. Digital detox aims to encourage time away from technological devices and screens, strengthen bonds among family members, and enhance social, emotional, and physical well-being.

Family Guide to Combating Gambling Addiction
The Family Guide to Combating Gambling Addiction aims to support effective responses to gambling addiction by explaining its risk factors, its economic, social, and psychological effects on individuals and family dynamics, and the recovery process. Its target audience includes individuals at risk of or experiencing gambling problems and their families, as well as other segments of society involved in combating addiction.

The guide highlights the effects of gambling addiction not only on individuals but also on family relationships, economic stability, and emotional well-being. It provides guidance to families on recognizing signs of addiction at an early stage; approaching affected family members with empathy, patience, and open communication rather than blame; setting healthy boundaries to protect themselves; seeking professional support; and taking an active and supportive role in the recovery process (Ministry of Family and Social Services, 2024). Within the scope of this report, the guide is also relevant to addressing gambling-related risks in the digital environment.

Parental Guide for the Protection of Children from Digital Risks
The Parental Guide for Protecting Children from Digital Risks was developed to support the protection of children from risks they may encounter in digital environments, increase parents' knowledge and awareness of digital parenting, and provide guidance on children's safe, conscious, and balanced use of digital technologies. The guide was published on the website of the Ministry of Family and Social Services (Ministry of Family and Social Services, 2025).

The guide addresses both the opportunities and risks associated with children's use of digital technologies and emphasizes the importance of digital parenting. It encourages parents to remain informed about technological developments, set appropriate limits on children's screen time, establish rules and provide guidance, and avoid leaving children unsupervised in online environments. It also emphasizes taking appropriate security measures, serving as positive role models in internet use, enriching children's time with off-screen activities, fostering awareness of digital privacy, avoiding the sharing of children's images and personal information on social media, and paying attention to children's digital gaming activities.

Guide to Protection from Cybercrime and Cyberbullying
The Guide to Protection from Cybercrimes and Cyberbullying was developed to support the protection of children from cybercrime and cyberbullying risks they may encounter in digital environments, increase children's and parents' knowledge and awareness of these risks, and provide guidance on how to respond appropriately and promptly in cases of risk or victimization. The guide provides recommended actions for responding to cybercrime and cyberbullying, as well as information on relevant institutions and reporting mechanisms. It is available on the website of the Ministry of Family and Social Services (Ministry of Family and Social Services, 2025).

"My Safe Internet" Storybook
The "My Safe Internet" storybook was developed for children aged 6–10 to introduce them to risks they may encounter in the digital world, convey basic rules for safe internet use, and provide parents with guidance on supporting their children. The book includes stories, activities, and mini-tests that inform children about the benefits and risks of internet use. Through a story centered on a journey into the digital world, the book introduces children to how the internet can be used for accessing information, entertainment, and learning. It also presents basic safety rules, such as avoiding communication with unknown persons, not sharing personal information, and accessing trusted content. In addition, the book provides guidance for parents on how to guide and support their children's internet use (Ministry of Family and Social Services, 2025).

Explore, Play and Learn with Children Guide
The "Explore, Play and Learn with Children Guide" was prepared by the General Directorate of Child Services of the Ministry of Family and Social Services to encourage families to spend quality time with their children, reduce screen dependency, and support children's development. The guide was published on the Ministry's website (Ministry of Family and Social Services, 2025).

Digital Safety Guide for Children
The "Digital Safety Guide for Children" was prepared by the Ministry of Family and Social Services to support the protection of children from risks they may encounter in digital environments and was published on the website of the General Directorate of Child Services. The guide addresses both the opportunities offered by information and communication technologies and the risks children may encounter in digital environments, using language and examples that children can easily understand.

The guide also provides basic information to help children develop safe behaviors on social media, digital games, and online platforms. It offers guidance on protecting personal information, matters to consider in online communication, and safe channels to use when encountering risky situations. In this context, the guide aims to empower children to protect themselves in digital environments, understand their rights and responsibilities, and engage in digital environments safely.

"My First Teacher, My Family" Mobile Application
The "My First Teacher, My Family" mobile application, developed by the Ministry of Family and Social Services, is a digital support platform designed to guide parents through their children's development. The application provides reliable, expert-supported content on child development, positive parenting skills, family communication, adolescence, and healthy family life.

Through the application, parents can track their children's development, access age-appropriate activities and recommendations, ask questions to experts, and receive interactive support. It also provides informative content on pregnancy, preparation for childbirth, and family life. Offered free of charge, the application aims to strengthen parents' informed parenting skills, support children's healthy development, and strengthen communication within the family (Ministry of Family and Social Services, 2026).

The educational, guidance, and information tools discussed above are summarized in Table 4.9 according to their target groups, primary areas of focus, and types of support.

Table 4.9 Selected Educational, Guidance and Information Tools for Families and Children

Programme / Tool	Target Group	Primary Focus	Type of Support
Türkiye Combating Addiction (TBM) Trainings	Ministry personnel, children aged 15+ in institutional care, general public	Technology and other behavioral addictions	Awareness and prevention
Family Education Programme / Modular Family Education Programme	Parents and families	Media literacy, internet use, social media, digital games and information technologies	Family education and digital/media literacy
Awareness Education Programme for Strengthening and Developing Children's Life Skills	Parents/caregivers of children aged 0–6; children aged 7–18 and parents for modules under development	Digital parenting, digital risks and children's life skills	Parental capacity-building and child education
Digital Detox Activities	Families	Screen use and family interaction	Balanced technology use and strengthening family bonds
Family Guide to Combating Gambling Addiction	Individuals at risk of or experiencing gambling problems and their families	Gambling-related risks and effects on family life	Awareness, early recognition and family support
Parental Guide for Protecting Children from Digital Risks	Parents	Screen time, privacy, online safety and digital games	Digital parenting guidance and prevention
Guide to Protection from Cybercrimes and Cyberbullying	Children and parents	Cybercrime and cyberbullying	Risk awareness, response guidance and reporting mechanisms
"My Safe Internet" Storybook	Children aged 6–10 and parents	Safe internet use, personal information and online interaction	Age-appropriate digital safety education
Explore, Play and Learn with Children Guide	Families with children	Screen dependency, family time and child development	Off-screen activities and family interaction
Digital Safety Guide for Children	Children	Social media, digital games, online platforms and personal information	Child-focused digital safety guidance
"My First Teacher, My Family" Mobile Application	Parents	Child development, positive parenting and family communication	Digital parental guidance and developmental support

Source: Compiled from the programmes, guides, and digital tools of the Ministry of Family and Social Services and relevant partner institutions discussed in this section.

4.1.2.4.2. Ministry of Interior (General Directorate of Security)

SİBERAY is an awareness programme implemented by the Department of Cybercrime of the General Directorate of Security under the Ministry of Interior to promote the safe, conscious, and beneficial use of the internet and technology. The programme provides training, seminars, and informative content on cybercrime, phishing and fraud, personal data protection, cyberbullying, technology addiction, and digital literacy, helping individuals recognize digital threats and take appropriate protective measures.

In this respect, SİBERAY contributes not only to combating cybercrime but also to strengthening preventive awareness before crime or victimization occurs. Through activities targeting schools, public institutions, social media, public transportation settings, and different age groups, the programme supports the development of a broader culture of digital safety across society.

4.1.2.4.3. Türkiye Radio and Television Corporation (TRT)

TRT provides a range of digital content, educational resources, and parental guidance tools aimed at supporting children and families in navigating the digital environment. Selected initiatives are summarized in Table 4.10 and described below.

Table 4.10 Selected TRT Digital Initiatives for Children and Families

Program / Tool	Target Group	Primary Focus	Type of Support
TABİİ / TABİİ Kids	Families and children	Family- and child-oriented digital content	Safe and age-appropriate digital content
TRT Kids Library	Pre-school and school-age children; parents	Digital reading and parental involvement	Child-oriented digital content and parental monitoring
TRT Kids Parent Academy	Parents	Screen time, digital games, online safety, digital addiction, media literacy and social media	Parental guidance and digital/media literacy
Digital Crew (Dijital Tayfa)	Children	Internet safety, personal data protection, cyberbullying, social media and technology addiction	Child-focused digital awareness and education

Source: Compiled from Türkiye Radio and Television Corporation (TRT), TRT Çocuk, and tabii resources.

TABİİ

Launched in 2023 under TRT's motto "Stories That Unite Us," TABİİ is an international digital platform developed as a domestic alternative to global digital platforms. It supports families' access to carefully curated, family-friendly content reflecting shared cultural values. The platform also includes content specifically presented as suitable for family viewing.

TABİİ Kids

TABİİ Kids offers a selection of content for pre-school and school-age children. It provides an ad-free digital content environment that takes account of pedagogical considerations, cultural values, and age appropriateness.

TRT Kids Library
TRT Kids Library is a digital library application for pre-school and school-age children. It supports children in developing safe reading habits in the digital environment and, through its parental panel, enables parents to monitor their children's reading and activity patterns.

TRT Kids Parent Academy
TRT Kids Parent Academy is a digital guidance platform for parents. It offers content on topics including child development, children and the media, digital awareness, family communication, and expert opinions, providing guidance to parents on screen time management, digital game selection, online safety, digital addiction, media literacy, and social media.

Digital Crew (Dijital Tayfa)
The Digital Crew series aims to promote conscious, safe, and responsible use of digital technologies among children through an engaging and child-friendly narrative. It addresses issues such as internet safety, personal data protection, cyberbullying, social media use, and technology addiction in language accessible to children. By combining educational messages with examples from everyday life, the series seeks to encourage children not only to acquire knowledge but also to act more consciously and responsibly in digital situations. In this respect, Digital Crew contributes to children's digital literacy and can also support family awareness of responsible technology use.

Radio and Television Supreme Council (RTÜK)
In addition to its regulatory role, RTÜK carries out media literacy and awareness-raising activities for children and families through educational publications, audiovisual content, and cooperation with the Ministry of National Education. Selected initiatives are summarized in Table 4.11.

Table 4.11 Selected RTÜK Media Literacy and Awareness Tools for Children and Families

Programme / Tool	Target Group	Primary Focus	Type of Support
RTÜK Media and Children Magazine	Children aged 9+	Media and digital literacy, technology awareness, cyber risks, disinformation, and social media	Child-oriented media literacy and accessible educational content
Nuclear Family (Çekirdek Ailesi) Animated Series	Pre-school and primary-school-age children; families	Advertising, time management, distinguishing fiction from reality, media effects, and access to accurate information	Age-appropriate media literacy and family awareness
Media Literacy Course and Educational Materials	Students in grades 7 and 8	Critical, informed, and safe engagement with media content	School-based media literacy education
Public Service Announcements and Outreach Activities	General public; children and families	Media literacy and awareness	Public awareness and outreach

Source: Compiled from Radio and Television Supreme Council (RTÜK) media literacy resources.

4.1.2.5. Concrete Instruments (Digital Monitoring, Parental Control Systems, etc.) and the Legal Framework of Oversight and Enforcement Mechanisms

Regulatory Framework for Social Media and Gaming Platforms
In 2026, Türkiye introduced new legislative provisions concerning social network providers and gaming platforms, strengthening the regulatory framework for the protection of children in digital environments. The relevant provisions are scheduled to enter into force on 1 November 2026 (Law No. 7578 on Social Services and Amendments to Certain Laws, 2026).

For social network providers, the framework prohibits the provision of services to children under the age of 15 and requires providers to take necessary measures, including age verification, to ensure compliance. For children aged 15 and above, providers are required to take measures to offer differentiated services specifically designed for children. Providers must also offer clear, understandable, and accessible parental control tools enabling parents to manage account settings, approve paid transactions such as purchases, rentals, and subscriptions, and monitor and limit usage time. In addition, providers are required to take measures against deceptive advertising (Law No. 7578 on Social Services and Amendments to Certain Laws, 2026).

For gaming platforms, the framework introduces requirements concerning age rating, parental controls, and, for certain foreign-based platforms, representation in Türkiye. Games that have not been duly rated may not be offered unless they are classified under the highest age category, while improperly rated content must be removed. Foreign-based gaming platforms receiving more than 100,000 daily accesses from Türkiye are required to appoint a natural or legal person as their representative in Türkiye, notify the relevant authority, and make the representative's contact information easily accessible. Gaming platforms are also required to provide parental control tools covering account settings and parental approval for paid transactions (Law No. 7578 on Social Services and Amendments to Certain Laws, 2026).

Information and Communication Technologies Authority (ICTA/BTK)

The Information and Communication Technologies Authority (ICTA/BTK), as the regulatory and supervisory authority for electronic communications and information technologies in Türkiye, also carries out initiatives aimed at promoting the safe, informed, and effective use of digital technologies. Its activities include awareness portals, guidance materials, training, research, and support mechanisms addressing issues such as safe internet use, digital privacy, cyberbullying, technology addiction, digital games, and digital parenting (Information and Communication Technologies Authority [ICTA], 2026).

Safe Internet Centre. Established within ICTA/BTK in 2016, the Safe Internet Centre promotes the conscious, safe, and effective use of internet technologies, particularly among children and young people. It brings together three complementary components—the Awareness Centre, Internet Help Centre, and Internet Information and Reporting Centre—covering awareness-raising, user assistance, and information and reporting functions. The Internet Help Centre also provides support through the Internet Help Portal and the Alo 141 Conscious and Safe Internet Use Support Line (ICTA, 2026).

Digital Games Information Platform and Guidance. ICTA/BTK also operates the Digital Games Information Platform (Güvenli Oyna) to promote informed, responsible, and safe engagement with digital games, particularly among children and young people. Related guidance includes the Privacy Guide for Digital Games, which draws attention to privacy and account-security risks in online gaming and provides practical recommendations for players and families on issues such as in-game communication, third-party links, application permissions, secure payment methods, personal data, and account protection (ICTA, 2026).

Radio and Television Supreme Council (RTÜK)

Smart Signs Protective Symbol System. The Smart Signs system is one of the concrete protective tools used by the Radio and Television Supreme Council (RTÜK) to provide viewers and parents with information on the age appropriateness of audiovisual content and potentially harmful content categories. In response to changes in the media environment, work is underway to update the system by expanding existing age categories and further developing content categories in line with emerging risks and needs (Radio and Television Supreme Council [RTÜK], 2026).

Presidency of Religious Affairs

The Presidency of Religious Affairs complements these initiatives through e-Diyanet and its television, radio, and children's broadcasting services. e-Diyanet provides families and young people with access to religious information and family guidance materials, including e-books, articles, and audio content addressing themes such as digital privacy, digital ethics, and family communication. Diyanet's children's broadcasting also provides child-oriented content through traditional and digital channels (Presidency of Religious Affairs, 2026).

Linkages with the Report's Value Framework

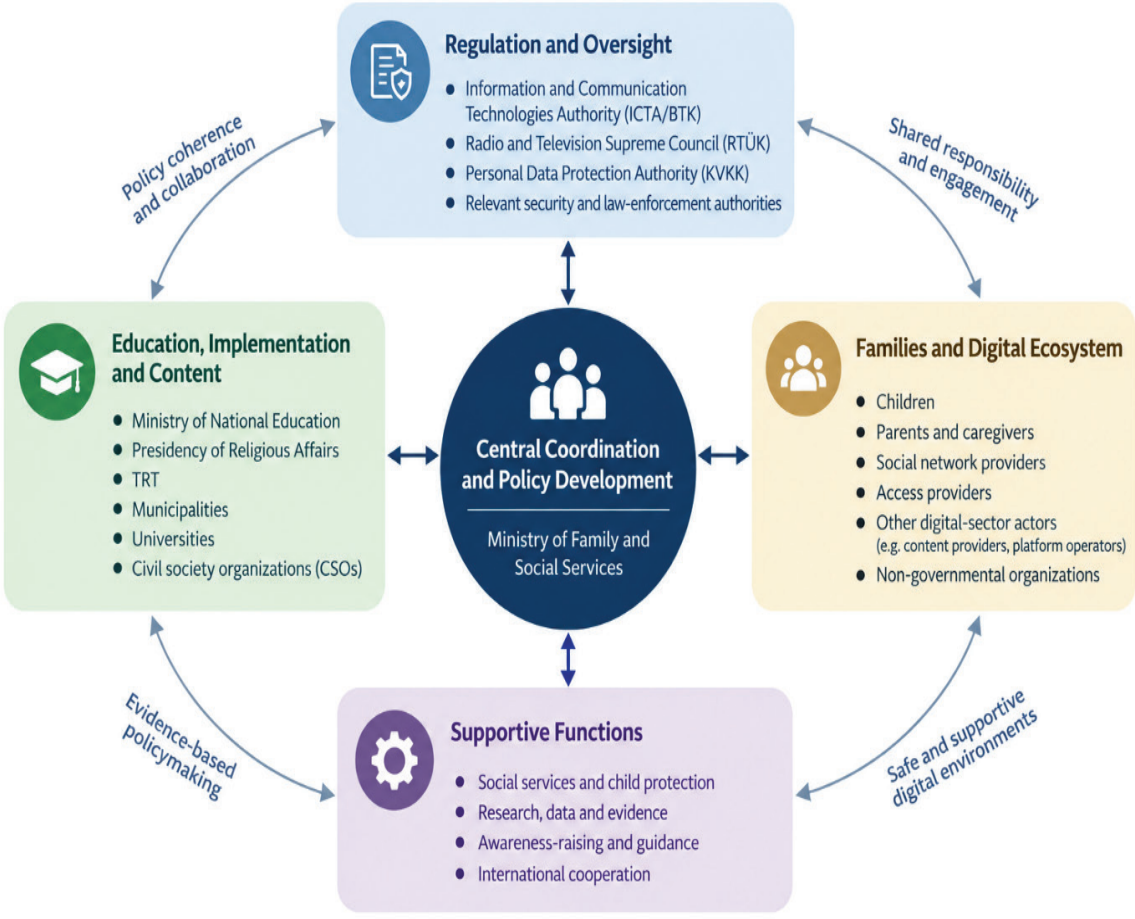
Viewed through the report's value framework, the strategy documents, action plans, regulatory measures, and institutional mechanisms examined in this section can be associated particularly with Hifz (protection of the family, progeny, and intellect) and Mas'uliyyah (responsibility). Measures aimed at protecting children in digital environments—including age-related safeguards, parental controls, content classification, media literacy, and digital safety guidance—illustrate different regulatory, educational, and family-support mechanisms through which the protection of children and families is pursued.

At the same time, the involvement of public institutions, families, media organizations, and digital service providers reflects a shared-responsibility approach to digital governance. From the perspective of the report's framework, this multi-actor structure is consistent with Mas'uliyyah, while the broader emphasis on safeguarding children and supporting families can be understood in relation to Hifz.

4.1.3. Institutional Structure and Governance

The governance structure for the protection of children and families in digital environments in Türkiye involves multiple institutions with complementary responsibilities in regulation, protection, education, content provision, and social support. The Action Plan for the Empowerment of Children in the Digital World (2026–2030) provides an overarching framework for this approach, bringing together public institutions as well as civil society organizations, social network providers, and access providers. In this way, the protection of children from digital risks is addressed across interconnected areas including social services, education, media regulation, personal data protection, security, technology, and digital content. The main actors and their complementary roles within this multi-stakeholder governance framework are illustrated in Figure 4.6.

Figure 4.6 Institutional Governance Framework for the Protection of Children and Families in the Digital Environment in Türkiye



Source: Authors' compilation based on the Action Plan for the Empowerment of Children in the Digital World (2026–2030) and the institutional sources examined in this section.

Within this structure, the Ministry of Family and Social Services plays a central role in coordination and policy development from the perspective of child protection and family policy. The Information and Communication Technologies Authority (ICTA/BTK) contributes regulatory and technical functions related to electronic communications and internet environments, complemented by mechanisms supporting safe and informed internet use. The Radio and Television Supreme Council (RTÜK) undertakes regulatory, monitoring, and awareness-raising activities related to the protection of children in broadcasting and media literacy, while the Ministry of National Education contributes through digital skills development and the promotion of safe technology use in educational settings. The Personal Data Protection Authority complements these functions through its role in the protection of children's personal data in digital environments.

The institutional framework also extends beyond regulatory and educational authorities. The Presidency of Religious Affairs contributes through family and child guidance and awareness-raising activities addressing issues such as digital technology use, privacy, and family communication. TRT complements these efforts through child- and family-oriented content and parental guidance. Together, these institutions illustrate how regulatory, educational, social, cultural, and content-related functions are distributed across different actors within the broader governance framework.

An important feature of this structure is the coordination of different institutional mandates around child and family protection. Reports concerning harmful content encountered by children in digital environments may, depending on their nature, involve different competent authorities, allowing social services, content regulation, technical intervention, and law-enforcement mechanisms to perform complementary functions. The International Policy and Practice Exchange on Child Protection in the Digital Environment, hosted by Türkiye in 2026, also brought together representatives of the public and private sectors, academia, civil society, and children, illustrating the broader multi-stakeholder dimension of this approach.

Overall, Türkiye's governance framework distributes regulatory, protective, educational, social-support, content-related, and awareness-raising functions among different actors while bringing them together around common strategic objectives. In particular, the Action Plan for the Empowerment of Children in the Digital World (2026–2030) provides a common policy framework involving children, parents, educators, professionals, public institutions, civil society organizations, and digital-sector actors. Continued coordination, information-sharing, monitoring, and cooperation among these stakeholders can support the effective implementation and further development of this multi-stakeholder framework.

Examples of Multi-Stakeholder Governance in Practice

An important feature of Türkiye's governance approach to protecting children in digital environments is the involvement of different stakeholders in policy-development processes. This approach brings together the regulatory and implementing roles of public institutions, the technical support of international organizations, academic expertise, the technical capacity of the private sector, the advocacy and monitoring functions of civil society, and the direct participation of children. Recent national and international meetings, workshops, and consultation processes provide concrete examples of how this multi-stakeholder approach operates in practice (Ministry of Family and Social Services [MFSS], 2026).

One of the most comprehensive examples is the International Policy and Practice Exchange on Child Protection in the Digital Environment, held on 21–22 April 2026. Hosted by the Ministry of Family and Social Services in cooperation with UNICEF and the Office of the United Nations Special Representative of the Secretary-General on Violence Against Children, the program brought together representatives from different countries and sectors. Multi-stakeholder roundtables addressed legal and policy frameworks for children's online safety, the role of the private sector in digital child protection, and the potential of digital technologies for children's empowerment and participation. A dedicated child and youth participation session also provided a platform for children to share their experiences, expectations, and proposed solutions. The program concluded with a joint outcome statement prepared in cooperation with the Ministry, UNICEF, and the Office of the UN Special Representative (MFSS, 2026).

At the national level, the Digital Addiction and Family Workshop and the Children in the Digital World Workshop, held in 2024, provide further examples of consultative policy development. The former brought together academics, civil society representatives, children, and parents, while the latter, organized in cooperation with UNICEF, involved representatives of public institutions, academia, digital content producers, and civil society. The workshops addressed digital risks and opportunities through complementary perspectives, including legal and regulatory issues, education and empowerment, and social awareness and support. Their findings and recommendations subsequently contributed to the preparation of the Action Plan for the Empowerment of Children in the Digital World (2026–2030) (MFSS, 2024, 2025, 2026).

Child participation constitutes another element of this governance approach. The 26th National Children's Forum, held in 2025 under the theme “Children's Rights in the Digital World,” provided a mechanism through which children from across Türkiye discussed online safety, personal data protection, cyberbullying, digital citizenship, and related issues and developed recommendations. The resulting declaration was subsequently presented by child representatives to the Speaker of the Grand National Assembly of Türkiye, providing a concrete channel for children's perspectives to reach decision-makers (MFSS, 2025).

Cooperation between civil society and public institutions provides another example. The Digital World Children's Rights Charter, initially developed as a civil society initiative, was subsequently presented to the public under the leadership of the Ministry of Family and Social Services and developed into a nationwide awareness campaign.

Activities were conducted across all 81 provinces, drawing on the outreach capacity of the Ministry's provincial directorates. By February 2026, the initiative had received 309,754 signatures, illustrating its broad public reach (MFSS, 2026).

These examples illustrate how multi-stakeholder governance in Türkiye is operationalized through consultation, knowledge and experience sharing, child participation, cross-sector cooperation, and the development of joint outputs. Continued links between consultation processes and policy monitoring and evaluation, together with information-sharing and sustained engagement with the private sector, academia, and civil society, can further support the continuity and effectiveness of this multi-stakeholder approach.

Linkages with the Report's Value Framework

Viewed through the report's value framework, Türkiye's multi-stakeholder approach to digital child protection can be associated particularly with Mas'uliyyah (responsibility) and Hifz (protection of the family, progeny, and intellect). The distribution of complementary roles among public institutions, families, educational actors, civil society, digital-sector actors, and children reflects an approach in which responsibility for children's well-being in digital environments is shared across different stakeholders rather than placed solely on families.

At the same time, regulatory safeguards, parental support mechanisms, digital and media literacy initiatives, child participation, and mechanisms for addressing harmful content illustrate different ways in which the protection of children and families is pursued in practice. From the perspective of the report's framework, these mechanisms can be understood in relation to Hifz, while the coordination and participation of multiple actors is consistent with the principle of Mas'uliyyah.

4.1.4. Implementation Mechanisms and Policy Instruments

Türkiye's approach to protecting children and supporting families in digital environments extends beyond legal and regulatory measures to include education and awareness-raising initiatives, technical safeguards, digital guidance and support services, and inter-institutional cooperation. These instruments address different dimensions of digital child and family protection, including capacity development, preventive protection, information, support, and early intervention. The selected practices below illustrate how these different policy objectives are translated into concrete implementation mechanisms.

Table 4.12 Selected Practices Supporting Digital Family Governance in Türkiye

Policy Objective	Practice in Türkiye
Education and capacity development	Family Education Programme (FEP)
Technical protection	Safe Internet Service
Information, support, and early intervention	Children Are Safe Platform

Source: Authors' compilation based on Ministry of Family and Social Services (2026) and Information Technologies and Communication Authority (2019).

Family Education Programme (FEP): Strengthening the Protective Approach Through Digital Parenting

The Family Education Programme (FEP) is one of Türkiye's comprehensive non-formal education programmes aimed at strengthening families' knowledge, skills, and awareness. The programme is continuously updated in response to changing societal needs, and in recent years, the effects of digitalization on family life have been systematically incorporated into its educational content. New modules addressing digital parenting, safe internet use, children's digital development, and online risks have become part of the programme's family education framework.

This approach complements child-focused technical safeguards by strengthening parents' capacity to understand digital environments, maintain trust-based communication with their children, and provide informed guidance. Implemented nationwide through a broad-based non-formal education model and reaching families from different socioeconomic groups, the programme provides an established mechanism for strengthening digital parenting capacity as part of broader family education and support.

Safe Internet Service and Safe Internet Centre: Dissemination of Technical Protection Mechanisms
The Safe Internet Service and Safe Internet Centre, operated under the coordination of the Information and Communication Technologies Authority (ICTA/BTK), are among Türkiye's key mechanisms for promoting safer internet use. Through the "Child Profile" and "Family Profile" options offered under the Safe Internet Service, families can set internet access preferences appropriate to children's needs and benefit free of charge from technical filtering tools designed to limit access to harmful content.

These technical safeguards are complemented by information and awareness-raising activities, training materials, and guidance provided through the Safe Internet Centre. This combination brings together technical protection with educational and guidance measures, supporting not only the restriction of access to harmful content but also the development of safer and more informed internet-use practices among children and families.

"Children Are Safe" Platform: Digital Guidance, Early Intervention and Access to Public Support Mechanisms
The Children Are Safe Platform is an integrated information and support mechanism developed in response to the effects of digitalization on family life. The platform provides comprehensive guidance to support parents in guiding their children more consciously in the digital world. It provides up-to-date information on children's privacy on social media, digital parenting approaches, effective use of parental control tools, technology addiction, online risks, the selection of safe digital content, and the opportunities offered by digital technologies.

The platform goes beyond its information function by providing an accessible support and referral mechanism for families and children. Through the website and application, users can access "Ask for Help" in cases involving neglect, abuse, violence, and peer bullying, as well as "Report Harmful Content" for harmful content encountered on social media, digital gaming platforms, and other online environments. Depending on the nature of the submission, cases are referred to Ministry specialists or the ALO 183 Hotline/ALO 112 Hotline, initiating the relevant assessment and intervention processes. In this way, the Children Are Safe Platform combines digital guidance with mechanisms that facilitate the early identification of risks, access to public support, and timely responses to problems encountered by children and families in digital environments.

Overall Assessment
An examination of Türkiye's digital family policies shows that implementation An examination of Türkiye's digital family policies shows that implementation mechanisms extend beyond the application of legal and regulatory measures to encompass a multilayered set of educational, technical protection, digital guidance, support, and participatory governance instruments. Within this framework, the Family Education Programme and the My First Teacher Is My Family Mobile Application aim to strengthen parents' knowledge and awareness of children's digital lives and their capacity to provide informed guidance. The Safe Internet Service complements these measures through technical safeguards, while the Children Are Safe Platform supports the early identification of digital risks, access to reliable information and guidance, and referral to appropriate public support mechanisms. These instruments illustrate a policy approach that combines preventive and protective measures with family support and guidance.

Overall, Türkiye's experience illustrates how regulatory measures, technical safeguards, family education, digital guidance, support mechanisms, and multi-stakeholder governance can be brought together within a family-centered approach to digital transformation. For OIC Member Countries facing similar challenges, the Türkiye case provides potentially relevant experience in combining different policy instruments, while the applicability of individual mechanisms will depend on national institutional, legal, social, and cultural contexts.

These tools illustrate a policy approach to addressing digital risks that combines preventive, protective, and supportive measures within a family-centered framework. By strengthening individual and family capacities while providing technical safeguards, guidance, and access to support mechanisms, this approach addresses different dimensions of the potential effects of digitalization on family life and children's safety. For OIC Member Countries facing similar challenges, Türkiye's experience offers potentially relevant examples of adaptable policy instruments and implementation mechanisms, while their applicability will depend on national institutional, legal, social, and cultural contexts.

Linkages with the Report's Value Framework

Viewed through the value framework of this report, the Türkiye case can be associated particularly with Hifz (protection of the family, progeny, and intellect) and Mas'uliyyah (responsibility). Measures aimed at protecting children and strengthening families' capacity to use digital technologies safely can be understood in relation to Hifz, while the distribution of complementary responsibilities among families, public institutions, and other stakeholders is consistent with Mas'uliyyah.

These linkages help situate the Türkiye case within the report's broader value framework, rather than implying that the policies examined were explicitly designed on the basis of these principles.

4.1.5. Challenges, Areas for Improvement and Key Takeaways

Türkiye has developed a range of policy documents, institutional mechanisms, and awareness-raising programmes aimed at protecting children and supporting families in digital environments. At the same time, the rapid evolution of digital technologies and online environments creates a continuing need for policies, implementation mechanisms, and institutional capacities to adapt to emerging risks and changing patterns of digital use.

One continuing challenge is the difference between the pace of technological change and that of policy and regulatory processes. AI-powered applications, generative AI systems, algorithmic content recommendations, and deep fake technologies can evolve and become widely used within relatively short periods, while policy and implementation frameworks generally require more time to adapt. Regular review and updating of existing frameworks therefore remain important for responding to emerging and evolving risks.

Effective institutional coordination is equally important given the cross-cutting nature of digital child protection. Responsibilities are distributed across the Ministry of Family and Social Services, the Information and Communication Technologies Authority (ICTA/BTK), the Radio and Television Supreme Council (RTÜK), the Ministry of National Education, the Ministry of Interior, the Ministry of Justice, and other relevant institutions. Building on the coordination mechanisms already established, continued development of information-sharing, joint monitoring, and inter-institutional coordination can support more integrated responses to multidimensional digital risks.

Differences in digital literacy and digital parenting capacity represent another important area for continued attention. Widespread internet access and digital device use do not necessarily translate into equivalent levels of knowledge among parents and caregivers regarding digital platforms, online risks, personal data protection, and safe internet use. Differences in digital skills between generations may also affect parents' ability to guide children's digital engagement. Extending digital literacy and guidance initiatives to parents and caregivers, alongside children, therefore remains an important component of family-centered digital policy.

The cross-border nature of digital platforms presents an additional implementation challenge. Social media platforms, online gaming services, and other digital services frequently operate across jurisdictions. Addressing harmful content, protecting children online, and implementing platform responsibilities therefore involve not only national regulatory frameworks but also international cooperation and sustained engagement with digital platforms.

Monitoring and evaluation provide another area for continued development. Systematic assessment of the reach and longer-term effects of awareness-raising activities, education programmes, and protective services can strengthen the evidence base for future policy development and help identify which interventions are most effective for different groups of children and families.

Looking ahead, emerging issues related to generative AI, deepfakes, algorithmic manipulation, evolving forms of cyberbullying and online fraud, and the protection of children's personal data are likely to require continued policy attention. Addressing these developments will involve not only technical and regulatory measures but also digital literacy, ethical awareness, digital citizenship, and family-based guidance and protection.

Ultimately, Türkiye has established a broad policy and institutional framework for protecting children and supporting families in digital environments. The key challenge for the coming period is to maintain the adaptability of this framework as technologies and digital practices continue to evolve. In this context, continued attention to institutional coordination, digital parenting capacity, international cooperation, and evidence-based monitoring and evaluation can support the further development of Türkiye's family-centered approach to digital transformation.

4.1.6. Lessons Learned from Effective Practices

1. **A Multidimensional Approach to Digital Child Protection:** Türkiye's experience illustrates the importance of combining regulatory and technical safeguards with education, parental guidance, psychosocial support, and awareness-raising. Digital child protection is therefore better addressed through complementary policy instruments rather than through technical restrictions or legal measures alone.

2. **Proactive Monitoring, Accessible Support, and Adaptive Policy Mechanisms**: Mechanisms such as the Social Media Working Group and the Children Are Safe Platform illustrate the value of connecting the identification of emerging digital risks with reporting, guidance, referral, and appropriate institutional responses. They also highlight the importance of maintaining policy mechanisms that can adapt to rapidly evolving technologies and online risks.

3. **Child and Family Participation in Policy Development:** National children's forums, consultation processes, and family-oriented programmes demonstrate the value of incorporating the perspectives of children and families into digital policy development. Such participation can help ensure that policy responses reflect the experiences and needs of their intended beneficiaries.

4. **Strengthening Family Capacity alongside Digital Safeguards:** Türkiye's experience highlights the complementary roles of digital parenting, media and digital literacy, parental controls, age-related safeguards, and child-sensitive digital environments. It also points to the value of knowledge-sharing and cooperation among OIC Member Countries in responding to rapidly evolving and cross-border digital risks, while allowing policy approaches to be adapted to different national contexts.

4.2. MALAYSIA

4.2.1. Introduction

Malaysia is a multi-ethnic and multi-religious country in Southeast Asia and one of the leading Member States of the OIC. Home to Malay, Chinese, Indian, and indigenous communities, the country has a Muslim Malay majority while maintaining a diverse social fabric. With a population of 36.6 million, Malaysia is also one of the region's most highly urbanized nations.

Despite this high urbanization, Malaysian society remains deeply committed to cultural traditions and Islamic values. A central element of this social fabric is the "Kampung spirit" (semangat kampung in Malay) - a cultural concept emphasizing that community members are collectively responsible for one another's well-being. Under this framework, raising children is not seen as the sole responsibility of the biological parents; instead, the extended family, neighbors, and the wider community share the duty of guiding a child's moral and social development. Consequently, the philosophy that "it takes a village to raise a child" remains a living reality across Malaysia.

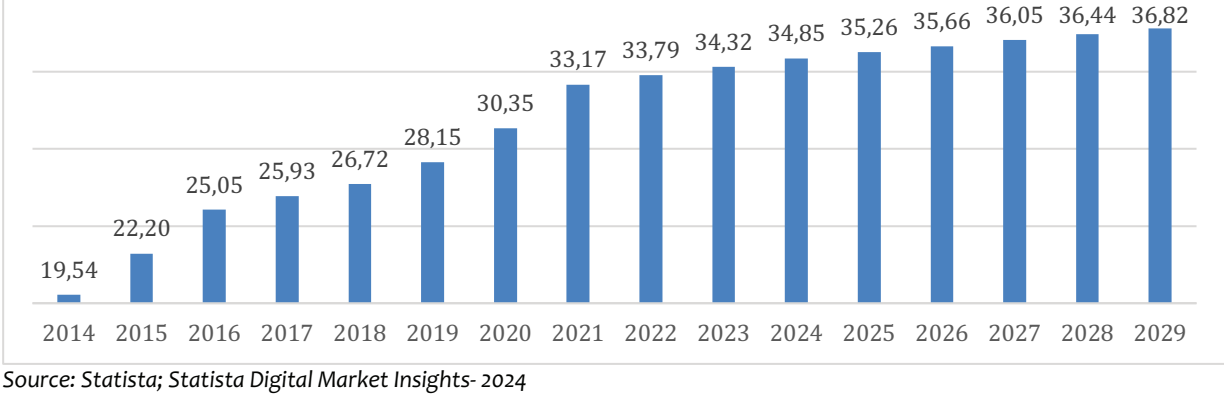
In Malaysia, the family structure extends beyond the nuclear unit to include the neighborhood and extended family. Within this community, living in accordance with religious values is a source of social prestige. Because the actions of individual family members affect the honor (maruah) of the entire family, young people grow up with a strong sense of self-control, both to avoid bringing dishonor to their family's name and to ensure they do not cross religious boundaries.

Although Malaysia remains committed to traditional values, global technological advancements have accelerated the country's digital and economic transformation, particularly in urban centers such as Kuala Lumpur, Selangor, and Penang. In recent years, Malaysia has made significant investments in the digital economy, artificial intelligence, mobile communications, and 5G infrastructure. This transformation is reshaping not only the economic landscape but also family relationships, parenting practices, concepts of privacy, and child-rearing methods.

The Malaysian government supports digital citizenship, digital literacy, and the online economy through strategic programs such as "MyDIGITAL" and the "Malaysia Digital Economy Blueprint." Digital technologies have become a fundamental part of daily life in the country. In particular, the widespread use of mobile internet has made Malaysia one of the most digitally engaged societies in Southeast Asia (Had & Ationg, 2026, p.643-644).

Figure 4.7 shows the steady increase in internet users in Malaysia, highlighting the country's rapid digital transformation and high level of digital connectivity. Widespread internet access has created a digitally connected society and laid the foundation for the growing use of digital technologies across different sectors and age groups.

Figure 4.7 Number of Internet Users in Malaysia (million)



Source: Statista; Statista Digital Market Insights- 2024

Younger generations, in particular, use digital technologies not only for communication but also for identity formation, education, socialization, entertainment, and economic activities. As digital technologies continue to evolve, the adoption of artificial intelligence (AI) tools is also increasing rapidly. According to a 2024 study, approximately three-quarters of Malaysians use AI tools in their daily lives (Telenor Asia, 2024, p.2).

Within this culturally diverse environment, digital transformation is significantly reshaping religious affiliation, cultural symbols, and family norms as users construct their digital identities. While this transformation positions the country as a regional hub for the digital economy, it also gives rise to new areas of social risk. In particular, children's digital safety, online privacy, cyber fraud, the spread of misinformation, and shifting dynamics in family communication are among the key areas of public debate in Malaysia.

Family Structure and Social Values

In Malaysian society, the family occupies a central place and serves as the primary institution for social well-being, cultural continuity, and value transmission. Particularly within the Muslim Malay community, it is viewed not merely as an individual, private unit, but also as a key social and religious institution responsible for transmitting values, preserving cultural identity, and fostering collective responsibility. Respect for elders, parental authority, strong family ties, and the protection of children remain central principles. As a result, family-related issues are generally perceived as matters of broader social importance rather than purely private concerns.

The process of digitalization is actively transforming these traditional family structures without fundamentally weakening their underlying values. Digital technologies have introduced new forms of communication, learning, and interaction within families (Had & Ationg, 2026, p. 643, 651). One notable example is the transmission of Islamic values through digital media. Religious education is no longer confined to mosques or formal institutions; online platforms such as YouTube, TikTok, and Instagram increasingly serve as channels for faith-based learning. Child-oriented digital content, including popular platforms such as "Omar & Hana," presents Islamic teachings in engaging and age-appropriate formats, demonstrating how digital technologies are being used to reinforce rather than replace traditional values (Ogilvy Malaysia, 2025).

Malaysia's multicultural and multi-religious society is also reflected in online behavior. Religious norms, cultural values, and social expectations continue to share digital interactions, while generational difference influence patters of technology use. Younger generations tend to maintain a stronger and more visible presence on social media, whereas older generations tend adopt a more cautious approach, placing a greater emphasis on personal privacy (Had & Ationg, 2026, p.643, 651).

These broader social changes are also transforming parenting practices. As highlighted in "The Future of Parenting" report, Malaysian parenting is gradually shifting from traditional authoritarian models towards more participatory and child-centered approaches, where children are increasingly involved in family decision-making. The report finds that 53% of Malaysian parents do not wish to replicate the strict disciplinary methods used by their own parents, reflecting changing expectations regarding parent-child relationships (Ogilvy Malaysia, 2025).

At the same time, parents remain highly concerned about the risks associated with children's digital lives, including cyberbullying, inappropriate content, online fraud, and privacy violations. While many families continue to rely on monitoring and screen-time restrictions, differences in parents' digital knowledge and skills may affect how effectively they are able to guide children's digital engagement. Consequently, the concept of "*enabling digital parenting*" has gained increasing prominence. Rather than relying solely on restrictions, this approach encourages parents to strengthen children's digital literacy, engage in shared online experiences, and develop children's long-term digital resilience (Mohamed et al., 2022, p. 26-27).

Research further shows that many Malaysian parents already adopt such practices to varying degrees. Approximately 76.9% warn their children about online risks, 71.6% set limits on screen time, and 70.4% discuss safe internet use with their children. Digital parenting experiences and capacities may nevertheless vary across households, including according to differences in income, education, and access to digital resources (Mohamed et al., 2022, p. 26-27).

These developments demonstrate that digital transformation has changed how Malaysian families communicate, educate, and support one another without fundamentally altering their core values. Rather than replacing traditional family-oriented norms, digital technologies have reshaped the ways in which cultural and religious values are transmitted across generations.

Level of Digitalization and Digital Usage Dynamics

Malaysia is among the most digitally advanced countries in the OIC, supported by widespread internet connectivity and near-universal smartphone ownership. According to 2024 data, smartphone ownership among Malaysian internet users stands at 99%, with 86% identifying the smartphone as their primary device for accessing the internet (Telenor Asia, 2024, p. 4). This high level of digital connectivity has positioned mobile technology as the main gateway to digital services and everyday activities.

Mobile internet has become deeply embedded in everyday life. Malaysians spend an average of 4 hours and 40 minutes online via mobile devices each day. Younger generations are particularly active online, with Gen Z users spending an average of 5 hours and 31 minutes per day on mobile internet. Digital technologies support a wide range of daily activities—from communication and financial services to education, work, and access to information—reflecting their integral role in modern Malaysian society (Telenor Asia, 2024, p.10).

Quick Fact:
How Malaysians Utilize Digital Tools

67% — Quick Information Access
63% — Mobile Payment Systems
61% — Online News Tracking
52% — Online Learning Activities

Source: Telenor Asia (2024, p. 10)

Social media plays a central role in maintaining personal and community relationships. Platforms such as WhatsApp, Facebook, Instagram, and TikTok are extensively used to communicate with family members, friends, and wider social networks. While younger users actively build their digital identities through these platforms, social media has also become an important space for information sharing, community engagement, and family interaction (Had & Ationg, 2026).

The rapid expansion of digital technologies has significantly influenced family life, particularly since the COVID-19 pandemic. Remote learning, working from home, digital parenting platforms, and online family communication have become part of everyday routines. At the same time, the adoption of artificial intelligence is increasing rapidly. Around 69% of Malaysian parents report using AI-powered parenting applications, while AI is more broadly employed for information gathering, problem-solving, creativity, and productivity. Public attitudes towards these technologies are generally positive, with around half of Malaysians expressing favorable views of AI (Ogilvy Malaysia, 2025, p. 11; Telenor Asia, 2024, p.15).

The growing integration of digital technologies has also transformed parental behavior on social media. Sharing children's photographs and developmental milestones online has become increasingly common, with 74% of Millennial parents regularly posting content about their children. This trend has contributed to growing discussions around children's digital footprints, consent, and the long-term implications of "sharenting" (Ogilvy Malaysia, 2025, p. 19).

Despite Malaysia's high level of digital adoption, concerns about cybersecurity and privacy remain widespread. Three-quarters of Malaysians report worrying about the security of their online accounts, particularly regarding identity theft, fraud, and personal data protection. Although 97% of users report using at least one privacy protection measure, many acknowledge that they lack a sufficient understanding of how these tools work in practice. This gap between technology use and digital literacy highlights the importance of strengthening digital awareness alongside continued technological advancement Telenor Asia, 2024, p.15).

Key Trends and Risk Areas

Digital transformation is reshaping family life and social interaction in Malaysia. Communication among family members increasingly takes place through digital platforms such as WhatsApp, Instagram, and TikTok. While these technologies strengthen connectivity and facilitate everyday communication, their growing use is also associated with changes in patterns of face-to-face interaction and has raised concerns about its implications for family relationships and social interaction (Had & Ationg, 2026, p. 650).

At the same time, digital platforms have created new forms of community support. WhatsApp groups, online parenting communities, and digital support networks have become important channels for sharing parenting experiences and maintaining family solidarity. Particularly in rapidly urbanizing areas, these platforms increasingly function as digital extensions of the traditional kampung (community) culture. This trend is reflected in the growing use of parental WhatsApp groups, which has increased by 75% since 2022 (Ogilvy Malaysia, 2025, p.7).

Social media has also influenced parenting practices and children's social experiences. The widespread use of Instagram and TikTok has encouraged the rise of "Instagrammable parenting," where parents frequently share children's lives online in search of social recognition. At the same time, children and young people face growing pressure to present carefully curated online identities, increasing the risks of social comparison, reduced self-esteem, and psychological stress (Ogilvy Malaysia, 2025, p.7; Had & Ationg, 2026, p.650).

Alongside these social changes, the spread of misinformation and algorithm-driven content has emerged as a growing concern. Recommendation algorithms often reinforce existing beliefs by exposing users to similar content, creating digital "echo chambers." This increases the risks of misinformation, social polarization, and public anxiety, as demonstrated during the COVID-19 pandemic when false information circulated widely through platforms such as WhatsApp and Telegram (Had & Ationg, 2026, p.650).

Cybersecurity and privacy have become major challenges accompanying Malaysia's rapid digital transformation. Between 2021 and 2024, more than 95,000 Malaysians suffered financial losses amounting to 3.18 billion Malaysian Ringgit (MYR) as a result of online fraud. Financial scams, phishing attacks, identity theft, data breaches, and the growing use of deceptive deep fake content represent some of the most significant digital threats. At the same time, many Malaysians report having little control over how their personal data are collected and used online. As children's digital engagement continues to grow, protecting children's privacy, strengthening parental control mechanisms, and promoting digital rights have become key policy priorities (Telenor Asia, 2024, p. 15).

These emerging challenges demonstrate that digital transformation requires not only technological innovation but also effective governance. In response, Malaysia has developed a comprehensive regulatory and institutional framework that combines legal measures, platform regulation, and preventive initiatives to promote a safer digital environment. The following section examines the main elements of this framework.

4.2.2. Regulatory Framework

A strong regulatory framework is essential for promoting digital safety, protecting users, and ensuring accountability in online environments. It establishes the legal and policy basis for responding to emerging digital risks while safeguarding children, supporting families, and fostering responsible digital practices.

This section examines the key components of Malaysia'a regulatory framework for digital governance and online safety, with particular attention to measures that promote a safer digital environment for children and families. It analyses national strategies, policy documents and legislation, regulatory tools for digital platforms and online content, the legal framework for regulatory oversight and enforcement, and the statutory integration of preventive measures such as education and awareness initiatives.

National Strategy, Policy Documents and Legislation

In recent years, Malaysia has embraced digital transformation as a primary driver of socioeconomic development, ensuring that this shift transcends purely economic and technological dimensions. By explicitly accounting for the profound impacts of digitalization on family structures, child development, and societal values, Malaysian government has systematically integrated its technology policies with broader goals of

social welfare and cultural sustainability. Reflecting the country's cultural and religious context, digital transformation strategies are guided by four complementary objectives:

- Economic growth,
- Social harmony,
- Preservation of moral values,
- Reinforcement of family well-being

In line with this approach, the Malaysian government has developed a multidimensional policy framework that integrates digital transformation with family and social development. National family policies, child protection strategies, digital economy plans, and communications regulations together provide the foundation for protecting families, children, and young people from digital risks while enabling them to benefit from technological opportunities.

Family policy has been a central component of Malaysia's social development agenda since the early 2000s. During this period, the family was formally recognized as a cornerstone of national development, leading to greater integration of family perspectives across public policies. The National Family Policy (Dasar Keluarga Negara) established the country's first comprehensive framework for strengthening marriage, promoting positive parenting, and supporting children's healthy development.

As digitalization accelerated and new social challenges emerged, Malaysia updated this framework through the National Family Compassion Policy (Dasar Keluarga Negara Kasih Sayang – DKKN). The policy positions the family as a key source of social resilience in the digital era and promotes stronger family relationships, parenting capacity, moral development, and digital literacy as strategic priorities (LPPKN, 2026).

A distinctive feature of the DKKN is its explicit focus on the multifaceted effects of digitalization on the household. The policy identifies excessive screen time, digital addiction, cyberbullying, online abuse, and social media-related risks as emerging threats to family well-being. In response, it promotes proactive digital parenting, lifelong family support, and digital literacy to help families adapt to an increasingly digital society. As shown in Table 4.13, the policy is implemented through the *KASIH Framework*, which translates its core family values into practical principles for strengthening family resilience in the digital era (LPPKN, 2026).

Table 4.13 The KASIH Framework of the National Family Compassion Policy (DKKN)

KASIH Principle	Core Value	Implication for Digital Families
K – Kasih Sayang	Love and Compassion	Fostering emotional support and empathy within the changing family structure
A – Akhlak	Moral Character	Preserving ethical boundaries and digital citizenship values online
S – Sihat dan Selamat	Health and Safety	Protects families from online and offline risks
I – Ilmu	Knowledge	Equipping families with critical information and digital literacy to adapt to technological change
H – Harmoni	Harmony	Promoting balanced digital practices that support healthy family relationships and positive interactions among family members

Source: Adapted from LPPKN (2026)

Complementing these family-focused policies, Malaysia's broader digital transformation agenda is guided by the *MyDIGITAL Initiative* and the *Malaysia Digital Economy Blueprint*, launched in 2021. These initiatives seek to transform Malaysia into a digitally driven, high-income nation by 2030 while promoting digital inclusion, cybersecurity, innovation, and public trust in digital technologies (Regulations. AI, n.d.).

Importantly, *MyDIGITAL Initiative* extends beyond economic development and technological advancement. It seeks to build a safe, secure, and inclusive digital society by promoting digital literacy and addressing the broader social impacts of digital transformation.

Within this framework, families are recognized as active partners in fostering responsible digital behavior and creating safer online environments, rather than simply as users of digital technologies. The strategy's key social priorities are summarized in box (Economic Planning Unit, Prime Minister's Department, n.d., p. 12).

MyDIGITAL Priorities Relevant to Families and Digital Inclusion

Digital Citizenship: Developing a robust culture of ethics, responsibility, and digital rights among users.
Literacy & Awareness: Promoting digital literacy and increasing parents' digital awareness to safely educate children.
Safe Environments: Creating secure online spaces and mitigating cyber risks.
Adaptive Support: Structurally supporting families and children in adapting to the realities of the digital economy.
Digital Inclusion: Enhancing universal access and facilitating digital service onboarding.

Source: Adapted from Economic Planning Unit (2021), Malaysia Digital Economy Blueprint, pp. 68–71.

These national strategies demonstrate that Malaysia's approach to digital transformation extends beyond technological advancement. By integrating digital development with family policy and social well-being, the country seeks to strengthen resilience at both the family and societal levels. Rather than relying primarily on restrictive measures, its policies focus on equipping families with the knowledge, skills, and capacity needed to engage with digital environments safely and responsibly.

Regulatory Tools for Digital Platforms and Content

As digitalization has gained momentum in Malaysia, online platforms, social media networks, and digital content providers have become critical components of national policies on families and children. Rising internet use among children and the growing role of digital technologies in family life have made the regulation of online content a key public policy priority.

The legal foundation of this framework is the ***Communications and Multimedia Act 1998 (Act 588)***. This Act consolidates the communications and multimedia sectors under a unified regulatory ecosystem, setting forth comprehensive principles regarding internet services, broadcasting activities, and digital content distribution (Communications and Multimedia Act, 1998).

The Malaysian Communications and Multimedia Commission (MCMC), the agency responsible for implementing the Act and overseeing digital platforms. In addition to its regulatory functions, the Commission develops policies and initiatives aimed at promoting a safer digital environment, particularly for children and families.

Complementing this legal framework, the *Malaysian Communications and Multimedia Content Code* serves as the principal self-regulatory instrument governing online content. It establishes ethical standards for digital media and provides practical guidance for industry actors in implementing responsible content practices.

Malaysia's digital governance framework is rooted in the principles of self-regulation and co-regulation, deliberately moving away from a conventional model of direct state censorship. This collaborative approach brings together publishers, digital platforms, internet service providers, and consumer representatives in the development and implementation of content standards. Consequently, digital content regulation is viewed not merely as an issue of media governance or freedom of expression, but also as a social policy instrument for safeguarding family well-being and ensuring children's online safety.

Legal Framework for Regulatory Oversight and Enforcement

While oversight and enforcement mechanisms play a significant role in Malaysia's approach to regulating the digital sphere, the overall system is based on a multi-stakeholder governance model rather than a centralized, top-down censorship framework.

At the core of this framework lies the ***Communications and Multimedia Act (CMA),*** Malaysia's principal legislation governing the communications and digital media sectors. Under the Act, the Malaysian Communications and Multimedia Commission (MCMC) monitors compliance with digital content regulations, investigates consumer complaints, and initiates enforcement or legal action where necessary (Communications and Multimedia Act, 1998).

To complement the CMA, Malaysia has introduced legislation addressing specific digital risks. A major development in this regard is the **Online Safety Act (OSA)**, which came into force in 2024. Rather than regulating individual users, the Act places primary responsibility on online platforms and service providers. Its objective is to enhance online safety by strengthening platform accountability and protecting users—particularly children—from harmful online content.

The First Schedule of the Act classifies harmful online content into five categories:

1. **Obscene Content:** Material that may cause public aversion due to immoral depictions or that systematically undermines a person's sense of decency and modesty.
2. **Inappropriate Content:** Digital media containing severe profanity or material that is starkly inconsistent with generally accepted societal behaviors and local cultural norms.
3. **Abusive Communication:** Content intended to cause systemic harassment, distress, fear, or psychological anxiety through threatening, profane, or abusive language and actions.
4. **Self-Harm Incitement:** Algorithmic or user-generated content that could directly or indirectly lead a child to engage in self-harming behaviors.
5. **Illicit Substance Promotion:** Media that encourages, facilitates, or promotes the illegal use, trafficking, or sale of dangerous narcotics and controlled drugs.

The scope of the Online Safety Act strictly applies to three key digital pillars, enforcing financial compliance penalties of up to 10 million Malaysian Ringgit (MYR) for non-compliant entities (Online Safety Act, n.d.):

- **Application Service Providers (ASPs):** Organizations offering software or digital services—such as social media networks or instant messaging platforms—that facilitate direct user communication over the Internet.
- **Content Application Service Providers (CASPs):** Entities providing targeted content services, including digital publishing platforms, streaming portals, or websites hosting user-generated media.
- **Network Service Providers (NSPs):** Infrastructure organizations that provide the physical network architecture and bandwidth, bound by the minimum statutory obligations defined under this Act.

Building on this framework, Malaysia introduced additional child online safety requirements that entered into force on 1 June 2026. These measures require digital platforms to incorporate child safety by design in line with the **Child Protection Code (CPC)**. They include age assurance measures for users under 16 and technical safeguards to reduce children's exposure to harmful interactions and inappropriate content (Malaysia Child Protection Code, 2026).

This regulatory framework is further supported by three complementary laws:

- **Computer Crimes Act:** Criminalizes cyber offences such as unauthorized access, data manipulation, and cyberattacks.
- **Personal Data Protection Act (PDPA):** Regulates the collection, processing, and protection of personal data.
- **Child Act:** Provides legal protection against child abuse, online grooming, and commercial exploitation.

These laws establish a comprehensive regulatory framework that combines enforcement with prevention. By integrating the **Communications and Multimedia Act**, the **Online Safety Act**, and child protection measures, Malaysia seeks to promote a safer digital environment through shared responsibility among regulators, digital platforms, service providers, and other stakeholders. This integrated approach supports online safety while strengthening the protection of children and families in the digital environment.

The Statutory Integration of Preventive Policies (Education and Awareness)

One of the strongest features of Malaysia's family and child safety framework is its emphasis on *prevention*. In this context, digital risk management is not based solely on sanctions or enforcement after harm occurs. Digital education, public awareness initiatives, and institutional capacity-building are treated as integral components of the broader social protection system.

Several of the policies discussed earlier are also important in this context because they incorporate preventive measures into Malaysia's digital governance framework. The National Family Compassion Policy (Dasar Keluarga Negara Kasih Sayang – DKKN) identifies family resilience and parental digital literacy as key national priorities, recognizing that parents need the knowledge and skills to guide children in digital environments (LPPKN, n.d.).

Similarly, the *National Child Protection Policy* seeks to reduce online risks before they affect children and families. To achieve this, the government implements safe internet use programmes, targeted digital awareness initiatives, and public campaigns addressing online harms. (Ministry of Women, Family, and Community Development, 2021)

MyDIGITAL Initiative also supports this preventive approach through structured digital literacy training for students, educators, parents, and older adults. In addition, practical guidance on digital parenting and online safety is provided through the Keluarga Bahagia Portal and the Family Coach Programs, which are implemented by the National Population and Family Development Board (LPPKN, n.d.).

By presenting these policies through the lens of education and awareness, this section highlights that Malaysia's regulatory approach combines enforcement with prevention. The framework seeks not only to respond to digital harm after it occurs, but also to build the knowledge, skills, and resilience needed to prevent harm before it emerges.

This integrated approach is reflected across Malaysia's major policy and legislative instruments. As summarized in Table 4.14, family policies, digital transformation strategies, and regulatory measures operate together to strengthen family well-being, promote digital literacy, and enhance online safety.

Table 4.14 Malaysia's National Policy and Legislative Framework for Families and Digital Transformation

Policy / Legislation	Purpose	Target Group	Family Dimension	Digitalization Dimension
National Family Policy (DKN)	Strengthen the family institution and improve family well-being.	Families, married couples, parents, children	Supports marriage, parenting skills and family cohesion.	Later complemented by digital parenting and media literacy initiatives
National Family Compassion Policy (DKKN) 2026–2030	Enhance family resilience in the digital age and preserve family values.	Families, parents, children, youth, elderly	Strengthens family communication and values.	Addresses digital addiction, screen-time management, digital parenting and online safety.
Child Act 2001	Protect children's rights and welfare.	Children, parents, caregivers	Ensures children grow up in a safe family environment.	Provides legal protection against online abuse, grooming and digital exploitation.
MyDIGITAL & Malaysia Digital Economy Blueprint	Accelerate digital transformation and economic development.	Citizens, businesses, students, public institutions	Supports family adaptation to digital transformation.	Promotes digital literacy, safe internet use and digital inclusion.
Communications and Multimedia Act 1998 (CMA)	Regulate communications and media sectors.	Platforms, broadcasters, ISPs, users	Provides the legal basis for regulating communications,digital media and online content.	Provides the legal framework for regulating online content and digital media.
Malaysian Communications and Multimedia Content Code	Establish ethical standards for digital content.	Content creators, broadcasters, advertisers, platforms	Limits content harmful to family values.	Defines content standards for children, age classifications and online safety principles.
Online Safety Act	Improve online safety and child protection.	Children, parents, teachers, users	Supports parents in managing children's online activities.	Requires online platforms to implement measures that protect users, particularly children, from harmful online content.

Source: Created by the Authors.

4.2.3. Institutional Governance Structure

Malaysia approaches digital transformation not only from the perspective of technological advancement and economic growth, but also as a strategic area for safeguarding the family institution, strengthening social resilience, and preserving cultural and religious values. In this regard, the country has adopted a multi-stakeholder governance model to address the challenges and risks associated with digital transformation.

This model is based on the coordination of institutions responsible for digital transformation, communications and cybersecurity, family-related policies, as well as bodies providing religious and ethical guidance. As a result, Malaysia views digital governance not merely as a technical or security issue, but as a comprehensive policy framework that supports family well-being and promotes social values in the digital age.

This section examines the institutional architecture underpinning this governance model by grouping the key institutions into three functional levels: (i) the Macro and Strategic Level (ministries and national committees), (ii) the Operational and Technical Level (specialised agencies), and (iii) the Regulatory and Enforcement Level, which oversees online safety, compliance, and the implementation of digital regulations.

4.2.3.1. Macro and Strategic Level (Ministry and Committees)

The principal institution responsible for the overall coordination of Malaysia's digital transformation is the ***Ministry of Digital*.** Established in December 2023 following a governmental restructuring, the Ministry serves as the central authority for formulating and implementing the country's digital transformation agenda, reflecting Malaysia's commitment to accelerating digitalization through a focused, holistic, and inclusive governance framework (Ministry of Digital, n.d.).

The Ministry is responsible for a broad range of policy areas, including the development of digital infrastructure, data governance, digital sovereignty, artificial intelligence governance, and the regulation of emerging technologies. It also seeks to ensure that the benefits of digital transformation are shared across all segments of society by promoting inclusive digital access, reducing digital literacy gaps, and strengthening public sector digital capabilities. Rather than viewing digital transformation solely as an economic driver, the Ministry also recognizes it as a process with significant social implications that should be managed in a sustainable and people-centered manner (Ministry of Digital, n.d.).

Since its establishment, the Ministry has introduced and coordinated several strategic initiatives aimed at strengthening Malaysia's digital ecosystem. These include the launch of the Digital First Strategy in 2024 to accelerate the digitalization of public services, the establishment of the National Artificial Intelligence Office (NAIO) in December 2024 to guide the development and governance of AI technologies, and the approval of the National Cloud Computing Policy in 2025 to enhance the country's cloud infrastructure and data management capabilities. In addition, amendments to the Personal Data Protection Act (PDPA) and the adoption of the Data Sharing Bill 2024 have strengthened the legal and institutional framework governing data protection, privacy, and responsible data sharing (Ministry of Digital, n.d.).

Within the scope of evaluating digital threats to the family institution, the institutional framework of Malaysia's Ministry of Digital demonstrates that, while there are no standalone masterplans or programmes explicitly dedicated to family protection, several of its strategic priorities contribute to creating a safer digital environment for families, children, and young people. Rather than addressing digital risks through family-specific interventions, the Ministry adopts a Whole-of-Government (WoG) approach that integrates technology governance, cybersecurity, education, and public awareness within a broader framework of social well-being (Ministry of Digital, 2024, pp. 6–7, 44, 54).

In this context, ***Cyber Resilience*** constitutes one of the Ministry's core strategic priorities. Efforts to strengthen cybersecurity include enhancing legal and regulatory frameworks, improving digital safety, and implementing public awareness programmes to promote cybersecurity and digital trust. The enactment of the Cyber Security Act 2024, together with amendments to the Personal Data Protection Act (PDPA), has further reinforced the institutional framework governing cybersecurity, data protection, and privacy in the digital environment.

At the societal level, the Ministry seeks to address digital risks through the Digital Society pillar, which focuses on digital literacy, ethical digital behavior, and equitable access to digital technologies. Initiatives such as the National Cyber Ethics (School Children Programme), CyberSAFE, AI for Rakyat, and the Digital Rakyat Portal aim to raise awareness of online safety, promote responsible use of technology, and strengthen digital literacy among citizens, including children and young people.

Although these initiatives are designed for society as a whole, they also contribute to strengthening the digital awareness and resilience of families by promoting safer and more responsible engagement with digital technologies (Ministry of Digital, 2024, pp. 6–7, 44, 54).

Accordingly, Malaysia's Ministry of Digital addresses the social dimensions of digital transformation not through family-specific policies, but through a broader ecosystem of digital safety, cybersecurity, digital literacy, and ethical technology use that indirectly supports families in responding to emerging digital threats (Bernama, 2021; Free Malaysia Today, n.d.; New Straits Times, 2026; University of Nottingham Malaysia, 2025).

The National Security Council (NSC) is the principal institution responsible for coordinating Malaysia's national security policies and strategic priorities. In the field of cyber security, the NSC plays a central governance role through the National Cyber Security Agency (NACSA), which operates under the Prime Minister's Department. (Cyber Security Act, 2024, Part II) This institutional arrangement reflects Malaysia's recognition of cyber security not merely as a technical issue but as an integral component of national security, economic stability, public safety, and societal resilience (Malaysia Cyber Security Strategy 2025–2030, n.d., pp. 16–17, 29–30).

The legal basis for this institutional framework has been further strengthened by the Cyber Security Act 2024 (Act 854), under which the National Cyber Security Committee is entrusted with determining national cyber security policies, strategies, and strategic measures. The Act also establishes the National Cyber Coordination and Command Centre System (NC4 System) as a national mechanism for managing cyber security threats and incidents in an integrated manner (Cyber Security Act, 2024). Although the primary focus of the NSC and NACSA remains on macro-level national security and safeguarding critical infrastructure, defining cybersecurity as an integral component of public safety and societal resilience provides the highest level of state guarantee and a robust legal shield for protecting families and young people from digital risks.

Alongside these macro-level security mechanisms, the ***Ministry of Science, Technology and Innovation (MOSTI)*** serves as a vital government institution responsible for leading Malaysia's science, technology, innovation, and economy (STIE) agenda. Throughout its institutional evolution, the Ministry has progressively expanded its responsibilities from science and technology governance to innovation, digital transformation, and technology-driven solutions that address national challenges and promote societal well-being. Its vision of building a high-tech nation is closely supported through research and innovation, technology development, capacity building, and the promotion of scientific knowledge across society (MOSTI, n.d.).

Within Malaysia's family-facing digital-resilience efforts, MOSTI supports grass-roots initiatives that translate broader technology policy into practical support for households. Platform KID (Keibubapaan Digital), launched in 2025 through collaboration among the International Islamic University Malaysia (IIUM), Youthopia, and MOSTI, responds to parental concerns about children's growing exposure to digital technologies by providing practical knowledge, ethical guidance, and tools for safe, healthy, and balanced use. Its significance for digital family governance lies in connecting high-level innovation policy with parent capacity and culturally grounded family support (International Islamic University Malaysia [IIUM], n.d.).

While the aforementioned ministries and security councils build the technological, regulatory, and educational infrastructure necessary to counter digital risks, the actual societal target of these efforts is managed directly by specialized social institutions. In this regard, the **National Population and Family Development Board (LPPKN)** serves as Malaysia's principal federal statutory body responsible for population and family development under the Ministry of Women, Family and Community Development. Originally established in 1966 as the National Family Planning Board under the Family Planning Act 1966, its mandate was expanded through the Population and Family Development Act 1984 (Act 352) to encompass population development, family development, and human reproduction. Since 2001, LPPKN has served as the lead national agency in these areas, supporting the formulation and implementation of family-related programmes and policies (IIUM, n.d.).

In addition to its policy and programme functions, LPPKN heavily contributes to evidence-based family governance through the FAMILY Repository, a specialized digital knowledge platform developed in collaboration with the Ministry of Women, Family and Community Development. This platform provides digital access to research papers, policy documents, legislation, and critical resources regarding family structures, population trends, and reproductive health.

Through these advanced digital functions, LPPKN not only supports the development of informed family policies but also provides the core institutional knowledge base required for addressing emerging social challenges, including the psycho-social and structural threats arising from digital transformation within contemporary Malaysian households (LPPKN, n.d.).

4.2.3.2. Operational and Technical Level (Specialized Agencies)

The National Cyber Security Agency (NACSA) is Malaysia's lead agency responsible for cyber security governance and coordination at the national level. Established in February 2017 under the National Security Council (NSC) within the Prime Minister's Department, NACSA is entrusted with strengthening the country's cyber resilience and coordinating national efforts to address increasingly complex cyber threats. Its mandate encompasses the development and implementation of national cyber security policies and strategies, the protection of National Critical Information Infrastructure (NCII), cyber threat response and coordination, cyber risk management, as well as cyber security awareness and capacity-building initiatives (NACSA, n.d.; Malaysia Cyber Security Strategy 2025–2030, n.d., pp. 5–7).

Within Malaysia's broader digital governance framework, NACSA adopts a comprehensive and whole-of-society approach to cyber security. The Malaysia Cyber Security Strategy (MCSS) 2025-2030 emphasizes that cyber resilience cannot be achieved solely through technical safeguards; rather, it requires strong governance, cooperation among public institutions, industry, academia, civil society, and informed communities. The Strategy explicitly promotes a Government-Business-Community (G-B-C) model and identifies community cyber resilience, public trust in digital ecosystems, and responsible digital citizenship as key strategic objectives (Malaysia Cyber Security Strategy 2025–2030, n.d., pp. 16–17, 29–30).

From the perspective of protecting families and society in the digital age, NACSA plays an important preventive and enabling role. Although the Agency does not implement family policies directly, its initiatives contribute to creating a secure digital environment in which families, children, and people facing higher access or protection barriers can safely participate in digital life. NACSA promotes cyber security awareness, encourages ethical online behaviour, and disseminates practical guidance for individuals and communities on issues such as phishing, scams, ransomware, identity theft, online fraud, and safe internet practices. Through these efforts, cyber security is framed not only as a national security concern but also as a societal responsibility aimed at strengthening social resilience and protecting the well-being of citizens in an increasingly digital society. In this regard, NACSA constitutes one of the core institutional pillars supporting Malaysia's efforts to safeguard not only its digital infrastructure but also the resilience and well-being of its communities and families in the face of emerging digital risks (NACSA, n.d.; Malaysia Cyber Security Strategy 2025–2030, n.d., pp. 42–57).

CyberSecurity Malaysia is the national cybersecurity specialist agency operating under the Ministry of Digital since January 2024. The agency is responsible for strengthening Malaysia's cyber resilience by providing a broad range of cyber security services, programmes, and initiatives aimed at reducing risks in digital systems and enhancing the country's capacity to respond to emerging cyber threats. Its activities cover cyber security responsive and proactive services, outreach and capacity-building programmes, strategic studies and engagements, as well as industry and research development. Through these functions, CyberSecurity Malaysia seeks to contribute to the development of a safer and more resilient cyber ecosystem that supports national security, economic prosperity, and social harmony (CyberSecurity Malaysia, n.d.).

The origins of CyberSecurity Malaysia date back to the establishment of the Malaysia Computer Emergency Response Team (MyCERT) in 1997, followed by the creation of the National ICT Security and Emergency Response Centre (NISER) to address information security issues at the national level. In 2007, NISER was rebranded as CyberSecurity Malaysia to reflect its expanded mandate in supporting the implementation of Malaysia's National Cyber Security Policy and addressing the growing complexity of cyber risks. Today, the agency adopts a forward-looking approach that combines cyber security services, research and innovation, public awareness, and talent development. Within Malaysia's broader digital governance framework, CyberSecurity Malaysia plays an important role in promoting cyber security awareness, strengthening digital trust, and enhancing the resilience of individuals, organizations, and society against evolving cyber threats (CyberSecurity Malaysia, n.d.).

4.2.3.3. Regulatory and Enforcement Level

The Malaysian Communications and Multimedia Commission (MCMC) is the principal regulatory authority established under the Malaysian Communications and Multimedia Commission Act 1998 to oversee the communications and multimedia sector in Malaysia. Its establishment was part of Malaysia's transition towards a convergence-based regulatory model in response to the rapid development and integration of telecommunications, broadcasting, and digital technologies during the late 1990s. Within this framework, MCMC occupies a central position in the country's digital governance architecture (MCMC, n.d.).

The Commission aims to promote broad access to communications and multimedia services, ensure affordable and quality services for consumers, facilitate transparent regulatory processes and fair competition, and strengthen collaboration between consumers, service providers, and industry stakeholders. Its regulatory framework encompasses four major dimensions: economic regulation, technical regulation, consumer protection, and social regulation (MCMC, n.d.).

Within Malaysia's digital governance framework, MCMC contributes to the protection of children and families primarily through its regulatory, enforcement, and public-awareness functions. Its activities include measures addressing cyberbullying, online harassment, harmful content, and the misuse of personal data and private imagery. Between January and October 2025, MCMC reported the removal of 27,704 cyberbullying-related posts following more than 35,000 complaints, compared with 8,756 posts removed in 2024 (Free Malaysia Today, 2025). The Commission has also engaged with digital platforms to address harmful content involving minors, submitting 1,578 content-removal requests between January 2022 and February 2026, with a reported 96 percent removal rate (The Sun Malaysia, 2026). Alongside these enforcement activities, MCMC supports preventive education and digital awareness through initiatives such as the Safe Internet Campaign. These activities illustrate the Commission's role in addressing online risks affecting children and families alongside its broader responsibilities for communications and multimedia regulation.

In parallel with these institutional and regulatory developments, the protection of children and families in the online environment has become an increasingly important policy area within Malaysia's digital governance framework. In this context, the Online Safety Act 2025 (Act 866), which entered into force on 1 January 2026, provides a legal framework for enhancing online safety by regulating harmful content and establishing duties and obligations for application service providers, content application service providers, and network service providers. (Online Safety Act 2025 [Act 866], 2025, §§ 1–3). The Act applies to online communication and content services operating within Malaysia and, under certain circumstances, beyond its territorial boundaries, reflecting a broad approach to addressing online risks and harmful content.

The Act also establishes ***the Online Safety Committee (OSC)*** as an advisory body on matters relating to online safety. The Committee consists of representatives from the ministries responsible for communications, home affairs, digital affairs, education, and women, family and community development, as well as representatives from the National Security Council, the Royal Malaysia Police, the Children's Commissioner, licensed service providers, persons with disabilities, and individuals with expertise in online safety. (Online Safety Act 2025 [Act 866], 2025, § 5). The Committee is responsible for advising and making recommendations to the Malaysian Communications and Multimedia Commission (MCMC) on issues such as the identification of harmful and priority harmful content, methods for analyzing and mitigating risks arising from harmful content, research on online harms, and best practices aimed at strengthening the accountability of service providers (Online Safety Act 2025 [Act 866], 2025, § 10).

The Act further includes specific provisions concerning the protection of child users. Licensed application and content service providers are required to implement measures to ensure the safe use of their services by children. These measures include preventing children's access to harmful content, limiting interactions between adult and child users, restricting features that may encourage excessive use of digital services by children, protecting children's personal information, and ensuring that personalized recommendation systems are suitable for child users (Online Safety Act 2025 [Act 866], 2025, § 18).

In conclusion, Malaysia has developed a multi-layered digital governance framework that combines digital transformation with the protection of families, children, and social values. Through a Whole-of-Government approach, strategic, technical, and regulatory institutions undertake complementary responsibilities in digital innovation, cybersecurity, family-oriented policies, and online safety.

This institutional framework demonstrates Malaysia's policy approach to addressing the social implications of digital transformation while supporting the protection of the family institution and a safer digital environment. The institutional architecture of this governance system is summarized in Table 4.15.

Table 4.15 Institutional Architecture of Digital Governance in Malaysia: Key Institutions by Functional Level

Functional Level	Institution / Agency	Affiliation and Core Relationships
Macro and Strategic Level	Ministry of Digital	The central authority for digital transformation policy; directly oversees CyberSecurity Malaysia
	National Security Council (NSC)	Coordinates national security policies; oversees NACSA via the Prime Minister's Department
	Ministry of Science, Technology and Innovation (MOSTI)	Leads the STIE agenda; collaborates with NGOs/Academia for grassroots digital resilience (e.g., Platform KID)
	National Population and Family Development Board (LPPKN)	Statutory body under the Ministry of Women, Family and Community Development; manages the FAMILY Repository
Operational and Technical Level	National Cyber Security Agency (NACSA)	Operates under the NSC; lead agency for national cyber security coordination and threat response
	CyberSecurity Malaysia	Technical specialist agency under the Ministry of Digital; focuses on cyber resilience, technical services, and outreach
Regulatory and Enforcement Level	Malaysian Communications and Multimedia Commission (MCMC)	Principal regulator for the communications and multimedia sector; enforces social regulation regarding harmful content
	Online Safety Committee (OSC)	Advisory body to MCMC; a multi-stakeholder committee including representatives from the NSC, Police, and the Ministries of Digital, Home Affairs, Education, and Women/Family

Source: Prepared by the authors based on official government sources.

While Malaysia's digital governance framework is built on a coordinated whole-of-government approach, its implementation depends on the active engagement of society as a whole. Government institutions provide strategic direction, the legal framework, and regulatory oversight, while families, educational institutions, civil society organizations, religious bodies, academia, industry, and digital platforms translate these policies into practice. This complementary whole-of-society approach has become a defining feature of Malaysia's efforts to strengthen digital literacy, promote online safety, and enhance family resilience. The following section examines the principal mechanisms through which these objectives are implemented.

4.2.4. Implementation Mechanisms and Policy Instruments

This section examines key implementation tools and policy practices adopted in Malaysia to strengthen the resilience of children, families, and society against digital risks. These initiatives contribute to the development of a safer, more informed, and ethically responsible digital environment.

Malaysia has introduced a range of programmes and practices that operate at different levels of digital safety governance, targeting children, parents, educators, and wider society. The following subsections analyze selected implementation tools as illustrative case studies within the Malaysian context.

4.2.4.1. Cyber Security Awareness for Everyone (CyberSAFE®) Program

Malaysia has adopted several awareness-based and preventive implementation tools to address digital risks affecting families and children. One flagship initiative is the CyberSAFE programme.

The program is primarily implemented by CyberSecurity Malaysia, the national cybersecurity specialist agency operating under the Ministry of Digital Malaysia. It is a public awareness program launched in 2010 to promote cybersecurity awareness among the general public and to foster a culture of safe and responsible digital usage. Its objectives include reducing risks in ICT systems, strengthening cyber security culture among users, and enhancing national human and technological capacities. (CyberSecurity Malaysia, n.d.). Beyond its technical cyber security objectives, CyberSAFE also functions as a preventive digital literacy and awareness mechanism aimed at strengthening broader societal resilience against online risks and to promote a safer digital environment for all (CyberSecurity Malaysia, 2024, p. 16).

Within this framework, Malaysia has implemented a range of practical measures aimed at strengthening public resilience against digital risks. These measures include online cybersecurity awareness courses, child online safety modules, personal data protection training, awareness campaigns on online scams and phishing attacks, and guidance on cyber incident reporting and response mechanisms. The programme also utilizes multilingual educational materials and modular training activities tailored to different social groups, including parents, students, and teachers (CyberSecurity Malaysia, 2023; UNICEF, 2020). The overall approach reflects a preventive and awareness-based governance strategy that prioritizes digital risk mitigation through education, public participation, and community engagement. In addition to cybersecurity awareness, CyberSAFE promotes digital literacy, media literacy, and cyber hygiene by encouraging responsible digital behaviour and safer internet practices.

Although CyberSAFE was not initially developed as a family-centered policy initiative, children, parents, students, and teachers constitute key target groups within the programme. As such, the initiative also contributes to family-oriented digital governance through child online protection, parental awareness, and the promotion of responsible digital conduct. In this respect, Malaysia's approach extends beyond a purely regulatory framework by combining awareness-building, literacy promotion, behavioral prevention, and collaborative governance mechanisms alongside technical cybersecurity measures. The program may be examined through five interconnected dimensions, each complementing and reinforcing each other.

a. Awareness Building and Preventive Governance

One of the key dimensions of the programme is its emphasis on awareness-building and preventive governance. Rather than focusing solely on responding to cyber incidents after they occur, the initiative prioritizes early prevention through digital awareness, safe technology practices, public education, and community outreach activities. (CyberSecurity Malaysia, 2023). This integrated approach introduces national strategies, awareness campaigns, and basic regulatory frameworks to reduce potential harm before it escalates. At the same time, it aims to improve public understanding of digital risks, including online fraud, privacy breaches, and harmful content. By incorporating preventive principles into public policy and institutional frameworks, the programme positions awareness as a key element of long-term digital governance and societal resilience (CyberSecurity Malaysia, 2023; NICTSED, 2025).

Overall, the approach combines awareness, education, and prevention with regulatory and technical measures to build a society that is more informed, responsible, and better prepared for digital risks.

b. Family and Child Protection

Families, and especially children, are among the most affected groups in the digital space. Although the programme was not originally designed as a direct family-focused initiative, children, parents, students, and teachers constitute key target groups within its implementation. It covers practical measures such as parental control tools, safe internet use practices, and age-appropriate content management. At the same time, it highlights the importance of strengthening communication within families so that digital risks can be understood and addressed collectively, rather than individually.

Under the broader CyberSAFE programme, Malaysia has introduced several thematic initiatives targeting families, youth and children. These include, among others, "CyberSAFE in School", "License2Surf", "CyberSAFE Parents" and interactive awareness platforms such as "the CyberSAFE L.I.V.E Gallery". Together, these initiatives aim to strengthen cyber awareness, promote responsible digital behaviour, and enhance online safety through education and preventive engagement.

One of the main initiatives under CyberSAFE is "CyberSAFE in Schools," which targets primary and secondary school students through awareness programmes, workshops, and online safety education. The initiative addresses issues such as cyberbullying, online grooming, privacy protection, social media ethics, and responsible internet use. It also involves teachers and parents through ambassador programmes, guidelines, and youth engagement activities (CyberSecurity Malaysia, 2023; UNICEF, 2020).

Another important initiative is "License2Surf," an interactive learning platform developed mainly for children and young internet users. The programme uses quizzes, games, videos, and simulations to teach topics such as password protection, phishing awareness, online scams, safe social networking, and privacy protection in a more engaging and accessible way (CyberSAFE Malaysia, 2023).

CyberSAFE also supports parental awareness through the "CyberSAFE Parents" platform. This initiative provides guidance and educational materials to help parents protect children from online predators, excessive internet use, cyber risks, and unsafe online interactions. It also encourages greater parental involvement in children's digital activities and online safety practices (CyberSAFE Malaysia, 2023).

In recent years, CyberSAFE activities have expanded through community outreach programmes and digital citizenship camps organized in cooperation with schools, non-governmental organizations (NGOs), telecommunication companies, and international organizations such as UNICEF. These initiatives aim to strengthen children's digital resilience and encourage safer, more responsible participation in digital environments (CyberSecurity Malaysia, 2023; UNICEF, 2020).

Consequently, the programme can be closely linked to family governance through dimensions such as child online safety, parental awareness, and the promotion of safe digital behaviour. By encouraging responsible online practices and strengthening awareness among both children and adults, the initiative indirectly supports families in navigating digital environments more safely and effectively. In this regard, the programme contributes not only to individual digital protection but also to the broader development of supportive and informed family-based digital governance practices.

c. Skill Development: Digital Literacy and Capacity Building

Awareness alone is not enough unless it is supported by practical skills. For this reason, this dimension focuses on building individuals' digital competencies through targeted training for parents, teachers, and children. These initiatives cover critical topics such as identifying misinformation, protecting personal data, and using digital tools safely. (CyberSecurity Malaysia, 2023). The broader goal is to strengthen the capacity of children and the adults who support them to benefit from digital opportunities while promoting safe, informed, and responsible participation in the digital environment (OECD, 2021a).

As a comprehensive framework for digital literacy, media literacy, and cyber hygiene, the CyberSAFE programme actively promotes responsible information use and safe online behavior. By helping users critically assess online content, protect their privacy, and develop healthy digital habits, the initiative fosters a more informed and resilient digital society (CyberSecurity Malaysia, 2023, pp. 14, 22–25; UNICEF, 2020a, p. 18).

Ultimately, CyberSAFE extends far beyond basic awareness-raising. It is designed to develop human capital, strengthen technical skills, and cultivate a secure digital culture. By equipping individuals and communities with sustainable competencies, the programme helps society adapt to rapid technological change while responding more effectively to emerging cyber risks and challenges (CyberSecurity Malaysia, 2023, pp. 14, 22–25; NICTSED, 2025, pp. 9, 53–56).

d.Response, Resilience, and Support Mechanisms

This dimension focuses on response, resilience, and support mechanisms when digital risks occur. Although prevention is important, online risks cannot be fully eliminated. Therefore, the key issue is how quickly and effectively incidents are addressed. The mechanism includes cyber incident reporting systems, coordination between institutions, and support services for affected individuals, including psychological and social assistance when needed. Strengthening these protective mechanisms helps reduce the impact of digital risks and improve societal resilience (CyberSecurity Malaysia, 2023, pp. 18, 20; OECD, 2021a, pp. 55, 58).

CyberSAFE's response capacity is driven by structured institutional cooperation and technical response functions operated under CyberSecurity Malaysia and its national Computer Emergency Response Team (MyCERT). Specifically, MyCERT manages the Cyber999 help centre, which enables users to report cyber incidents and receive immediate technical assistance. Beyond incident management and real-time threat monitoring, MyCERT coordinates strategic responses with government agencies, Internet Service Providers (ISPs), and international CERT networks. This collaborative structure ensures timely intervention and a more effective handling of complex cyber risks (CyberSecurity Malaysia, 2023, pp. 18, 20; MyCERT, 2024, p. 7; OECD, 2021).

Overall, these coordinated mechanisms help limit the impact of cyber incidents and accelerate the recovery process. By maintaining robust response systems, the programme contributes to a safer, more stable, and resilient digital environment for both individuals and communities.

e. Multi-Stakeholder Collaboration and Digital Ecosystem

Digital risks cannot be managed by a single institution alone. For this reason, this dimension highlights the importance of cooperation among governments, private sector companies, civil society organizations, educational institutions, and international partners. This collaborative framework encompasses joint awareness programmes, real-time information sharing, and coordinated policy efforts designed to elevate digital safety and cybersecurity awareness globally (ITU, 2022, p. 45; OECD, 2021, p. 62).

In the case of CyberSAFE, cooperation between government agencies, schools, communities, and technical institutions plays a central role. The active involvement of these diverse entities demonstrates a comprehensive, whole-of-society governance approach aimed at strengthening long-term societal digital resilience. By cross-linking different sectors, the programme successfully promotes shared responsibility, strengthens public participation, and establishes a sustainable infrastructure for responsible online behavior (CyberSecurity Malaysia, 2023, p. 28; UNICEF, 2020, pp. 12–15).

In short, the initiative recognizes that digital safety depends not only on top-down regulations and technical measures, but also on strong coordination and cooperation across the entire digital ecosystem.

These five dimensions provide a structured but flexible framework for strengthening cybersecurity awareness and family digital resilience. Rather than addressing digital risks separately, the approach connects prevention, protection, digital capacity, response mechanisms, and multi-stakeholder cooperation in a more integrated way (ITU, 2022, p. 50; OECD, 2021, p. 65).

Beyond its technical cybersecurity functions, CyberSAFE serves as a comprehensive digital literacy and awareness initiative that aims to strengthen societal resilience. Through school programmes, community-based activities, and public education efforts, the program promotes responsible digital behaviour, online safety awareness, and safer internet practices. In this respect, the programme goes beyond conventional cybersecurity approaches by emphasizing prevention, awareness, and digital risk reduction at the societal level (CyberSecurity Malaysia, 2023, p. 32; UNICEF, 2020, p. 25).

Studies on digital safety initiatives in Malaysia suggest that interactive learning tools and long-term public engagement activities are generally more effective than one-time awareness campaigns. However, research also underscores that bridging the gap between basic awareness and long-term behavioral change remains a critical challenge in developing sustainable digital habits among users (OECD, 2021, p. 68; UNICEF, 2020, p. 28).

Overall, Malaysia's approach represents more than a purely regulatory model. It combines awareness, digital literacy, behavioral prevention, and technical cybersecurity measures within a broader governance framework. This approach reflects a whole-of-society strategy that aims to build digitally resilient, informed, and responsible communities (CyberSecurity Malaysia, 2023, p. 35; ITU, 2022, p. 53). From the perspective of digital family governance, the programme represents a preventive and awareness-based policy instrument that supports safer digital engagement for children, parents, and society at large. In practice, CyberSAFE contributes to broader value-oriented governance principles such as protection, responsibility, prevention of harm, and ethical digital conduct in online environments.

4.2.4.2. Click Wisely (Klik Dengan Bijak- KDB) Program: "Pause, Think and Click!"

Launched by the Malaysian Communications and Multimedia Commission (MCMC) in 2012, the "Click Wisely" (*Klik Dengan Bijak*–KDB) initiative stands as one of Malaysia's foundational digital awareness programmes. The framework was developed to foster safer, more ethical, and responsible internet practices among the general public, anchored by four core pillars: security, alertness, responsibility, and the positive use of digital technologies (MCMC, 2023, pp. 12–14). In practice, the campaign champions conscious digital behavior, urging users to reflect carefully before clicking, sharing, or interacting online.

Within the framework of Malaysia's digital family governance, KDB integrates cybersecurity education with efforts to promote ethical technology use across children, parents, and the broader community (MCMC, 2023, p. 15). To maximize its societal reach, the initiative deploys a diverse array of educational tools, including school workshops, multimedia campaigns, interactive quizzes, and practical guide materials. Through these tools, participants engage with critical online safety topics such as cyberbullying, privacy protection, digital reputation, financial scams, and smart parenting practices. Beyond technical online safety, the programme also emphasized ethical digital behavior, family responsibility, and the development of a more responsible digital culture within society (ASEAN ICT Forum, 2024, p. 8; MCMC, 2023, p. 16).

A defining characteristic of the KDB framework is its emphasis on continuity. Rather than relying on sporadic, one-time campaigns, awareness activities are systematically integrated into schools and community centers to sustain public engagement and support the long-term development of safe online habits (MCMC, 2023, pp. 18–21). Furthermore, the initiative heavily focuses on enhancing social media literacy and responsible digital participation among younger people. In collaboration with local educational institutions, KDB designs tailored workshops that equip youth and parents with the critical thinking skills needed to engage with the contemporary media landscape safely and responsibly (UNICEF, 2020, pp. 34–36).

At the operational level, the campaign promotes highly practical safety principles, summarized by its flagship maxim: *"Pause, Think, and Click."* This straightforward rule advises users to verify links, downloads, and information before engaging, thereby mitigating the risks of online fraud and structural cyber threats. (MCMC, 2023, pp. 22–24). Additionally, the campaign underscores the critical importance of data protection, encouraging users to actively manage their privacy settings and remain vigilant about the personal information they share on social media platforms.

The programme can be examined through the following dimensions:

a. Child and Family Digital Awareness

The Program raises awareness about online risks affecting children, including cyberbullying, online grooming, harmful content, privacy risks, and unsafe online interactions. Through school-based programmes, workshops, and awareness campaigns, the initiative encourages children and young internet users to adopt safer online practices and become more aware of digital risks (MCMC, 2023, p. 25; UNICEF, 2020, p. 34). By promoting responsible social media use and safer communication habits, Click Wisely supports broader child protection efforts through preventive education rather than relying solely on regulatory measures.

A central focus of this dimension is strengthening family digital literacy and active parental guidance. The initiative covers critical areas relevant to contemporary households, such as online gaming safety, digital reputation management, and smart parenting practices. Parents are encouraged to become more actively involved in their children's online environments and to better understand emerging digital threats. To support this, the programme provides practical educational materials and structured guidance on balancing

excessive screen time, managing home privacy settings, and mitigating cyber risks (MCMC, 2023, pp. 26–28). It also underscores the importance of shared family responsibility in cultivating a safe digital culture. By enhancing parental awareness, the initiative aims to build protective home environments and strengthen long-term family resilience against digital risks.

b. Media Literacy and Responsible Online Behavior

A foundational pillar of the Click Wisely framework is the cultivation of media literacy across different layers of society. The initiative equips users—particularly children, students, and families—with the critical thinking skills required to evaluate online information and verify digital content before trusting or sharing it. Awareness activities focus heavily on identifying fake news, detecting online scams, recognizing manipulated multimedia content, and avoiding irresponsible social media behavior (MCMC, 2023, p. 30; OECD, 2021, p. 45). By strengthening these analytical habits, the programme enhances digital literacy and helps households engage with contemporary media environments with greater safety and discernment.

Parallel to content evaluation, Click Wisely places a strong emphasis on digital ethics and accountable online citizenship. Users are encouraged to communicate respectfully, abstain from spreading harmful materials, and recognize the real-world social consequences of their digital footprints. Rather than relying solely on external content monitoring, the framework champions positive peer interaction, emotional self-regulation, and responsible participation in digital spaces (MCMC, 2023, pp. 32-34). It systematically addresses structural challenges such as cyberbullying, online harassment, and harmful digital interactions. Through these educational interventions, the programme goes beyond basic safety checklists to foster value-oriented digital principles and a healthier online culture nationwide.

c. Community Based-Awareness and Collaborative Governance

The programme is carried out in cooperation with government agencies, private sector organizations, non-governmental organizations (NGOs), universities, and international partners. By coordinating with schools, local community hubs, universities, and telecommunication providers, the programme organizes synchronized awareness campaigns, practical workshops, and local community activities. This extensive network significantly broadens the reach of digital safety education among students, educators, parents, and local citizens alike (MCMC, 2023, p. 38). Such a collaborative structure reflects a comprehensive, whole-of-society governance approach, positioning digital safety not as an isolated regulatory duty, but as a shared responsibility across families, educational bodies, public authorities, and the wider digital ecosystem.

As a whole, the Click Wisely programme serves as a family- and community-centric framework that blends child online protection, parental active guidance, media literacy, and ethical digital conduct into a cohesive digital citizenship model.

Table 4.16 KDB Key Performance Indicators (2012-2024)

10,000,000+	Total Individuals Engaged: Reached through multifaceted campaigns, educational workshops, and grassroots outreach strategies.
1,372	Targeted Programmes Executed: Dedicated campaigns systematically delivered to schools, community centers, and families.
84%	Average Comprehension Score: Achieved by participants engaging with the specialized *MyCyberGenius* online safety module.
100,000~	Social Media Followers: Cultivating a robust, continuous digital footprint across primary social media channels.

Source: ASEAN ICT Forum, 2024

Between 2012 and 2024, Click Wisely reached more than 10 million people through awareness campaigns, educational workshops, and public outreach activities (Table 4.15). It also built a strong online presence, attracting nearly 100,000 followers across its social media platforms.

During this period, the programme implemented 1,372 cyber safety initiatives, while participants in the MyCyberGenius online safety module achieved an average score of 84%. These outcomes demonstrate the programme's important contribution to strengthening digital literacy and cyber awareness in Malaysia.

The programme also addressed a broad range of online risks affecting children, parents, and communities, including child online protection, cyberbullying, sexting, online grooming, and problematic internet use. By promoting parental controls, encouraging open parent–child communication, and supporting healthy screen-time management, Click Wisely has strengthened family-centered digital safety and responsible online behaviour.

4.2.4.3. Platform KID (Platform Keibubapaan Digital): A Case of Value-Based Digital Parenting Support

Parallel to state-led initiatives, Platform KID (Platform Keibubapaan Digital) represents an important academic initiative within Malaysia's digital parenting ecosystem. Developed by researchers at the International Islamic University Malaysia (IIUM) with funding from the Ministry of Science, Technology and Innovation (MOSTI), the platform was created to help parents address the everyday challenges of raising children in the digital age.
A distinctive feature of Platform KID is its integration of practical online safety guidance with local cultural and Islamic values, responding to the strong demand among Malaysian parents for faith- and value-based parenting resources (Mohamed et al., 2025, p. 996). Rather than serving as a conventional information portal, the platform combines educational materials, expert advice, and peer support within a single digital environment.

Through bilingual content, short videos, infographics, quizzes, live Q&A sessions, and community engagement, Platform KID enables parents to strengthen their digital parenting skills while supporting children's safe and responsible use of technology.

Empirical Basis of the Platform

Platform KID was developed on the basis of nationwide surveys and focus group discussions with Malaysian parents. The findings revealed that many parents struggle to regulate screen time, identify harmful online content, and respond to digital risks, largely because of differences in their own levels of digital literacy. Although parents expressed a strong commitment to protecting their children, many lacked the confidence and practical skills needed to do so effectively. The research also highlighted a clear preference for parenting resources that combine digital education with ethical and religious guidance. In particular, 83.2% of respondents preferred content grounded in Islamic values and traditional Eastern cultural principles, demonstrating that digital parenting in Malaysia is shaped not only by concerns about online safety but also by deeply rooted moral and cultural values (Mohamed et al., 2025). Platform KID integrates educational resources with interactive and community-based support to help parents address the challenges of raising children in the digital age. Rather than functioning as a conventional information portal, it provides practical, user-oriented guidance that supports parents in their everyday digital parenting practices (Platform KID, n.d.).

Platform KID: Strategic Vision and Accessibility

Official Portal: Platform KID provides free, nationwide access to digital parenting resources through its online platform:

https://platformkid.my

🎯 Official Tagline: *Building Roots for the Growth of a Smart and Balanced Digital Generation*

Key Strategic Vision: Reflecting its tagline, Platform KID aims to **"build roots"** by nurturing the values, knowledge, and digital habits that support healthy, balanced, and responsible relationships between children, families, and technology. This approach views online safety as a long-term process of character and capacity building rather than simply a set of technical safeguards.

The platform was developed through an iterative design process that incorporated user feedback. Early evaluations found that users considered the initial prototype overly static and insufficiently engaging. In response, the platform introduced more interactive features and personalized support mechanisms.

Participants particularly valued functions such as age-based content filtering, personalized recommendations, automated reminders, chat functions, and direct access to expert consultation, highlighting the importance of continuous engagement in encouraging parents to use the platform on a regular basis (Mohamed et al., 2025, pp. 1009–1010).

Core Features of Platform KID

Age-Appropriate Frameworks: Parents can filter guides and advice based on their child's specific developmental age group.

App-Specific Guides: Tips and parental control advice tailored to popular applications (like YouTube, TikTok, or gaming platforms) that children frequently use.

Expert Insights & Support: The platform integrates advice from local Malaysian experts, including digital communication lecturers, child health specialists, and clinical psychologists.

Interactive Diagnostic Tools: Features like the "Dapatkan Nasihat Khas" (Get Special Advice) tool allow parents to input their specific household situations and receive tailored strategies.

Parent Community: Opportunities to ask experts questions, exchange experiences, and learn from other parents.

Source: Authors' synthesis based on publicly available Platform KID materials and Mohamed et al. (2025).

Integrated Value-Based Digital Parenting Framework

Platform KID operationalizes an integrated digital parenting framework that shifts parental mediation from reactive monitoring towards a more proactive and developmental approach. Within the platform, digital parenting is conceptualized as a multidimensional process that harmonizes child safety, behavioral development, and value-based guidance. Rather than focusing only on control mechanisms, the platform brings together digital competence, moral awareness, and parental support as interconnected elements of children's online experiences (Mohamed et al., 2025, 994; p. 1001).

Child Online Protection (Value-Based Safety Dimension)

Within Platform KID, child online protection is structured around both technical safety and value-based awareness. The platform directly addresses critical household challenges, including screen time management, exposure to harmful content, cyberbullying, and privacy risks, which many parents report struggling to manage due to limited digital literacy and low technological confidence (Mohamed et al., 2025, p. 1011). Through interactive and child-friendly tools, the platform actively elevates awareness regarding safe internet utilization and fosters age-appropriate digital behaviors (Mohamed et al., 2025, p. 1001, 1003).

In this dimension, online safety is not limited to technical protection. Instead, it is explicitly linked to moral awareness and cultural responsibility, positioning safe digital navigation as an extension of ethical conduct within both the family unit and broader society.

This initiative directly operationalizes Malaysia's national regulatory focus on child online protection. While recent statutory frameworks introduce increasingly strict mandates, such as independent age-verification requirements and comprehensive child safety codes (ECPAT/UNICEF, 2022, p. 12; UNICEF, 2022, p. 34), their macro-level enforcement depends heavily on localized parental awareness and capacity. Platform KID complements these regulatory measures by providing educational and value-based support that helps parents translate broader online-safety principles into everyday digital parenting practices.

Digital Citizenship and Responsible Behavior

Platform KID also integrates digital citizenship and responsible online behavior as a core dimension. The findings show that parents associate digital parenting with moral development and character formation, explicitly expecting children's online behavior to reflect values such as respect, responsibility, empathy, and moderation (Mohamed et al., 2025, p. 1009).

To reinforce these expectations, the platform actively promotes digital engagement through interactive learning tools such as videos, quizzes, and practical activities. These modules support children in developing digital literacy while also encouraging respectful communication, awareness of privacy, and ethical participation in digital environments (Mohamed et al., 2025, 1009–1010).

Parental Mediation and Family Support

Parental mediation and family support form a core dimension of Platform KID. Research shows that while parents deeply intend to protect their children online, parents may differ in their confidence and capacity to manage digital risks effectively (Mohamed et al., 2025, p. 1008). Consequently, they often rely on reactive strategies like strict device restriction, which offer short-term control but fail to build long-term digital resilience (Mohamed et al., 2025, p. 1011).

To bridge this enforcement gap, Platform KID promotes an enabling mediation approach. Instead of rigid restrictions, it empowers parents to guide children through open communication, awareness-building, and shared learning. This methodology encourages children to become active, responsible participants in digital spaces, helping them develop independent judgment over time (Mohamed et al., 2025, p. 1003).

Platform KID also adopts a structured approach to content development, aimed at translating expert knowledge into accessible and practical guidance for parents. Its content development framework organizes information around the age and developmental needs of children, relevant digital risks, concise educational messages, and practical guidance for parental responses. Table 4.17 presents the key elements of this approach as reflected in the Platform KID content guidance.

Table 4.17 Key Elements of Platform KID's Content Development Approach

Content Element	Purpose
Target Age Group	To adapt content to children's developmental stages and age-specific digital risks.
Digital Risk or Concern	To provide a concise explanation of the relevant online risk or behavioral concern.
Concise Educational Message	To communicate key guidance in an accessible format suitable for visual educational materials.
Parent–Child Communication Guidance	To provide practical guidance for communicating with children about digital challenges.
Practical Action Steps	To suggest household practices, behavioural responses, or technical safety measures that parents can apply.

Source: Authors' synthesis based on publicly available Platform KID materials and Mohamed et al. (2025).

Beyond the structure of its content, Platform KID also places digital parenting guidance within a broader cultural and value-based framework. Its approach combines practical support with culturally appropriate communication and ethical and Islamic values, including *hikmah* (wisdom), *adab* (proper conduct), and *amanah* (trust and responsibility). While Table 4.16 focuses on how parenting content is structured and communicated, Table 4.18 highlights the broader principles that guide this approach.

Table 4.18 Key Dimensions of Platform KID's Value-Based Approach to Digital Parenting

Dimension	Main Focus	Relevance for Digital Parenting
Family Centered Practical Guidance	Translating digital parenting guidance into accessible and actionable forms	Supports parents in responding to everyday digital challenges through practical guidance rather than relying solely on restrictive approaches.
Cultural Responsiveness and *Adab*	Adapting digital parenting guidance to Malaysia's cultural and family context	Encourages approaches that are sensitive to family relationships, cultural norms, and appropriate conduct in digital environments.
Value-Based Digital Engagement	Connecting digital behavior with ethical values such as *amanah*, *hikmah*, and *adab*	Encourages responsible technology use, self-regulation, respectful online behavior, and awareness of individual responsibility in digital spaces.

Source: Authors' synthesis based on publicly available information on Platform KID.

Platform KID illustrates how digital parenting support can combine practical guidance with culturally and ethically grounded approaches. By linking digital safety and responsible technology use with values such as *adab* and *amanah*, the initiative provides a useful example of how digital literacy interventions can be made more relevant to everyday family life and local cultural contexts.

Integrated Perspective

Across all three dimensions, Platform KID embeds a strong value-based orientation. The platform consistently integrates moral, cultural, and Islamic principles into its digital parenting framework, ensuring that technological adaptation aligns with traditional family structures. (p. 114). Consequently, foundational values such as respect, modesty, responsibility, and empathy are positioned as central components of modern digital citizenship rather than isolated ethical considerations.

Overall, Platform KID operationalizes this integrated framework by combining technical competence, digital literacy, and value-based guidance within a single structure (Mohamed et al., 2025, p. 1001). Empirical findings indicate that digital parenting becomes more effective when it moves beyond technical safety measures and incorporates interactive learning, family engagement, and culturally grounded value systems (Mohamed et al., 2025, p. 1010).

The Platform KID illustrates how empirical evidence can directly inform the development of a user-centred and culturally responsive digital parenting platform. Its design is grounded in field-based research and continuously strengthened through user feedback from parents, children, and young people, ensuring that the platform remains dynamic and closely aligned with evolving user needs.

The success of Platform KID is closely linked to its strong empirical foundation and its adaptive structure, which allows for ongoing improvement based on real user experiences. The researches suggest that the long-term effectiveness of digital parenting initiatives depends not only on the provision of informational content, but also on the creation of an interactive and participatory digital community. In this regard, the integration of interactive design elements, gamification strategies, and community-based engagement mechanisms is essential for sustaining user interest and enhancing platform effectiveness over time (Mohamed et al., 2025, p. 1010).

4.2.4.4. A Comparative Analysis of Digital Family Governance Initiatives in Malaysia

Table 4.19 presents a comparative overview of three key digital family governance initiatives in Malaysia: CyberSAFE, Click Wisely, and Platform KID. The comparison highlights that while all three initiatives aim to strengthen digital safety and responsible online behavior, they operate at different levels within the broader governance ecosystem. CyberSAFE primarily focuses on technical cybersecurity awareness and risk prevention, whereas Click Wisely emphasizes digital citizenship, ethical behavior, and media literacy. In contrast, Platform KID introduces a more integrated and family-centered approach by combining parental mediation, child development, and value-based (including cultural and Islamic) guidance.

Table 4.19 A Comparative Analysis of Digital Family Governance Initiatives in Malaysia

Dimension	CyberSAFE	Click Wisely	Platform KID
Primary Focus	Cybersecurity awareness and risk prevention	Digital citizenship, ethical online behavior, media literacy	Value-based digital parenting and family-centered guidance
Target Group	Students, general internet users	Youth and general public	Parents and families (primary), children (secondary)
Core Orientation	Technical safety and risk mitigation	Behavioral awareness and ethical digital use	Holistic parenting support (safety + literacy + values)
Governance Structure	Government-led multi-agency initiative	Government + communication agencies + partners	University-led research-based initiative (IIUM)
Institutional Design	Policy/implementation-driven	National awareness programme	Research-to-policy platform (academic + applied design)
Sustainability Model	State-supported, campaign-based	Long-running national programme	Evolving platform (feedback-driven development)
Engagement Strategy	Awareness campaigns, trainings	Repeated national campaigns, school outreach	Interactive tools (videos, quizzes, Q&A, peer sharing)
Behavior Change Mechanism	Awareness → risk avoidance	Awareness → ethical digital citizenship	Values + parenting mediation → long-term behavioral shaping
Child Agency	Low–moderate (user as recipient)	Moderate (behavioral guidance)	Higher (interactive participation, feedback, shared learning)
Parental Role	Indirect	Limited / awareness-based	Central (active mediation role)
Values Integration	Low explicit value framing	Moderate ethical framing	High (Islamic + cultural + moral integration)
Cultural Adaptation	General safety framing	Context-sensitive messaging	Strong localization (values + culture + religion)
Technology Level	Low–moderate (campaign tools)	Moderate (digital campaigns, media tools)	High (interactive platform design)
Evidence Base	General policy-driven design	Communication strategy-based	Strong empirical foundation (surveys, focus groups)
Key Added Value	Cyber risk protection	Ethical digital citizenship	Integrated value-based digital parenting model

Source: Created by the Authors.

To sum up, the comparative analysis highlights that Malaysia's digital family governance initiatives operate through complementary but distinct layers, combining technical cybersecurity measures, behavioral guidance, and value-based family support. While this multi-layered structure strengthens the overall ecosystem, the effectiveness of these initiatives is also shaped by several implementation realities on the ground. These practical limitations and challenges are discussed in the following section.

4.2.5. Implementation Challenges and Areas for Further Strengthening

Within the Malaysian digital ecosystem, despite the broad implementation of digital safety initiatives such as CyberSAFE, Klik Dengan Bijak, Platform KID, and other child online protection programmes, several factors remain relevant to the effective implementation and reach of these interventions. The Malaysian case is particularly informative given the country's rapidly expanding digital adoption and the continuing need to ensure that children and families are equipped to respond to evolving digital risks.

One area requiring continued attention is supporting parents and caregivers in effectively guiding children's digital engagement. Evidence from Malaysia indicates that children continue to encounter harmful online experiences and highlights the importance of strengthening parents' and caregivers' digital literacy and capacity to support children online (UNICEF, 2020; UNICEF & ECPAT, 2022, pp. 6–7). This highlights the importance of sustaining educational and family-support measures alongside awareness-raising efforts to help translate knowledge into safer digital practices.

Another important dimension is coordination among the multiple stakeholders involved in digital safety. Malaysia's child online protection ecosystem involves government agencies, civil society organizations, educational institutions, and private-sector actors. While this multi-stakeholder structure brings together diverse capacities and expertise, effective coordination and cooperation across actors remain important for ensuring coherent and sustainable implementation (UNICEF & ECPAT, 2022).

More broadly, Malaysia operates within a rapidly evolving digital environment in which technologies, patterns of use, and associated risks continue to change. The Malaysian experience therefore illustrates that the effectiveness of digital safety initiatives depends not only on the availability of programmes and regulatory measures, but also on sustained engagement, accessibility, coordination, and the capacity to respond to evolving risks. This underlines the importance of continuously adapting digital parenting and child online protection initiatives as the digital environment evolves.

4.2.6. Lessons Learned

Beyond specific policies and programmes, Malaysia's approach reflects a broader recognition that effective engagement with technology requires not only technical solutions but also attention to responsible and ethical use. This is evident in the emphasis placed across the initiatives examined in this case on digital literacy, responsible technology use, online safety, and support for families in the digital environment. This broader approach is also consistent with the view that scientific and technological progress should be guided by ethical values and a clear sense of purpose rather than by technical considerations alone (Bakar, 2014). Within the value-based framework of this study, this perspective can be related to the principles of hikmah and amanah, particularly their emphasis on wise judgement, moral responsibility, and the purposeful use of technology.

In this context, the Malaysian experience offers several interconnected lessons for digital family governance:

1. **Institutional Framework: Combining Whole-of-Government Governance with Whole-of-Society Implementation**

Malaysia's experience highlights the importance of coordination among institutions responsible for digital transformation, cybersecurity, communications, family affairs, and child protection. This whole-of-government approach is complemented by the engagement of families, schools, academia, civil society, religious institutions, industry, and digital platforms in digital literacy and online safety. The key lesson is that protecting children and strengthening families in the digital environment requires both institutional coordination and broad-based participation.

2. **Regulatory Framework: Combining Legal Protection with Shared Responsibility**

Malaysia also demonstrates the value of a multi-layered regulatory framework rather than reliance on a single legal instrument. Its approach combines communications and cybersecurity regulation with child protection, platform responsibilities, and preventive measures. This suggests that digital family governance can be strengthened when legal protection is complemented by shared responsibility among public authorities, digital platforms, families, and other stakeholders.

3. **Strategic Orientation: Shifting from Enforcement to Preventive Education**

Malaysia's approach extends beyond regulation and enforcement by placing sustained emphasis on awareness-raising, digital literacy, and preventive education. Initiatives implemented through schools and communities illustrate the value of continuous engagement rather than one-off campaigns. This preventive orientation can help strengthen digital safety practices and build longer-term resilience among children and families.

4. **Cultural Anchoring: Integrating Cultural and Ethical Values into Digital Policy**

A key lesson from the Malaysian experience is the importance of grounding digital interventions in the cultural and social contexts of families. While national initiatives promote responsible digital behaviour, online safety, and child protection, Platform KID provides a more explicit example of integrating values such as *adab* (proper conduct), *amanah* (trust and responsibility), and *hikmah* (wisdom) into digital parenting support. Together, these experiences suggest that digital policies can become more relevant to families when technical measures are complemented by culturally grounded and value-based approaches.

CyberSAFE, Klik Dengan Bijak, and Platform KID illustrate the complementary dimensions of Malaysia's approach. CyberSAFE emphasizes cybersecurity awareness and risk prevention; Klik Dengan Bijak promotes responsible digital citizenship and media literacy; and Platform KID adds a more explicit family-centred and value-based parenting dimension. Their complementary functions illustrate how technical safety, responsible digital participation, and parental guidance can collectively contribute to a broader approach to digital family governance.

4.3. JORDAN

4.3.1. Introduction

The Jordanian Constitution recognizes the family as the basis of society and associates it with religion and morality (Hashemite Kingdom of Jordan, 1952/2022). For this report, that normative foundation is translated into governance questions: whether digital services strengthen rather than fragment family life, protect children's development and rights, preserve privacy and dignity, and allocate responsibility clearly across institutions.

Against this normative background, Jordan provides a relevant case for examining the interaction between digital public infrastructure, family policy, and child protection within a multi-stakeholder governance setting. Its young population, high urbanization, and diverse household circumstances provide an important context for services delivered at scale through multiple channels. The analysis covers two complementary dimensions: the digital threats experienced by families and children, and the governance and service arrangements in place to prevent and respond to harm. The access, trust, prevention, and intervention framework connects these two dimensions.

Jordan's digital transformation has increasingly emphasized digital public infrastructure based on shared digital identity, electronic signatures, data sharing, payments, and one-stop services. SANAD, Jordan's digital government services platform, provides access to digital identity and a range of public services. Alongside this digital infrastructure, the Personal Data Protection Law, hybrid service centers, the National Council for Family Affairs' (NCFA) family-policy coordination, the Ministry of Social Development's social services, the Public Security Directorate's Family and Juvenile Protection Department, the Jordan River Foundation's (JRF) support and referral capacity, and child-centered research address different dimensions relevant to families and children. Taken together, these elements provide a basis for examining the links between digital infrastructure, family policy, and child protection (World Bank, 2024a, 2024b; Tullis, 2025; NCFA, 2024; Jordan River Foundation, n.d.-c).

Jordan's connectivity indicators are high. According to the 2024 Household Survey on Information and Communication Technology Use and Access published by the Ministry of Digital Economy and Entrepreneurship (MoDEE), 96.5% of households have internet access at home, individual internet use stands at 95.6%, and daily internet use at 94.8%. By contrast, computer use stands at 34.7% (MoDEE, 2026a). These are access and use indicators for the survey's defined populations, not measures of digital safety or family well-being. Meaningful inclusion also requires purposeful use, appropriate devices, practical skills, accessible services, and the ability to obtain help.Jordan has also developed an evidence base on children's online experiences and related risks. The NCFA-UNICEF national study and Save the Children Jordan's research involving both children and parents provide insights into the risks experienced by children, levels of adult awareness, and the help channels available to and used by children (NCFA & UNICEF Jordan, 2021; Save the Children Jordan, 2024). Such evidence can inform preventive measures and support mechanisms, including awareness-raising, parental guidance, school-based support, and reporting and referral services.

For analytical purposes, the Jordan case is examined through four complementary functions: (1) access through digital public infrastructure and hybrid service channels; (2) trust through data protection, cybersecurity, and user rights; (3) prevention through family information, digital literacy, and child-protection measures; and (4) intervention through reporting, counseling, referral, case management, and remedy. This functional approach allows the analysis to consider how different policies and institutions relate to families' everyday interactions with the digital environment.

This case study is a documentary review of legislation, official institutional materials, published studies, and programme reports, supplemented by written technical comments from Jordanian stakeholders. It is not a new national survey or an evaluation based on direct service-user interviews. Publication dates, fieldwork periods, populations, and source types are distinguished below. Institutional descriptions reflect documented responsibilities; proposed areas for further development are presented as analytical suggestions rather than as additional institutional mandates.

Jordan's published policy framework places digitalization within a broader quality-of-life and user-centered reform agenda, rather than treating it solely as an expansion in the number of digital transactions. The Economic Modernization Vision and the Public Administration Modernization Roadmap connect service reform with quality of life, institutional integration, accountability, and results-oriented performance (Government of Jordan, 2022; Ministry of Planning and International Cooperation, 2022). Accordingly, this case considers access, service continuity, family well-being, child protection, privacy, and families' ability to use services safely and effectively, including where access or support barriers exist.

Family Structure and Social Values

In Jordanian society, the family is an important institution through which economic solidarity, care, identity, religious and moral education, and social belonging are supported. Extended kinship ties, intergenerational support, and respect for elders retain their importance despite urbanization and the growth of nuclear households. The Jordanian Constitution recognizes the family as the basis of society and associates it with religion and morality, reflecting the importance accorded to the family within the country's legal framework (Hashemite Kingdom of Jordan, 1952/2022). From the perspective of digital family governance, this supports consideration of the family not merely as a target of regulation but also as an important actor in prevention, guidance, and support.

Jordan's population includes citizens as well as long-term residents, migrants, and refugee communities, creating diverse household circumstances and service needs. Jordan's 2025 Digital Inclusion Policy and the World Bank's recommendations on digital public infrastructure emphasize inclusive access to digital identity and public services (MoDEE, 2025a; Tullis, 2025). For families, access to health, education, social assistance, and documentation services is particularly relevant to everyday well-being and participation. Complementing digital channels with government service centers and face-to-face support can also facilitate access for older people, users with limited digital skills, and families with substantial caregiving responsibilities.

Digital communication can enable Jordanian families to sustain relationships of care, financial support, and everyday decision-making among geographically dispersed family members. Messaging applications, video calls, family groups, and online money transfers can facilitate communication and support across distance.

More broadly, research on digital family life highlights the importance of household practices such as communication, shared rules, and parental guidance in shaping how technology affects family relationships (Livingstone & Blum-Ross, 2020).

In the context of childrearing, parental responsibility and child protection provide an important dimension of family life and policy in Jordan. In digital environments, this responsibility can extend beyond prohibition or surveillance to include active mediation, co-use, role modeling, age-appropriate autonomy, and a trust-based culture of help-seeking. Research on digital parenting highlights the importance of parental guidance, communication, and shared engagement in children's digital lives (Livingstone & Blum-Ross, 2020). These considerations are relevant to family- and child-focused awareness and guidance initiatives in Jordan.

One issue relevant to family-level digitalization is that children, parents, grandparents, and other caregivers may develop digital knowledge and confidence at different rates. Such differences are not merely technical: they can affect families' ability to establish shared rules, discuss online experiences, recognize manipulation or harm, and seek help early. This makes intergenerational digital guidance relevant not only at the household level but also to broader family-support policies, linking family support, schools, community communication, and trusted referral channels.

The family is therefore a unit of analysis in its own right. Relevant outcomes include the quality of parent–child communication, shared time, agreed rules for adults and children, privacy between family members, and confidence in seeking help without blame. Caregivers may gain easier contact with schools and services while experiencing new pressures to supervise use. These experiences may vary depending on factors such as age, disability, income, geographic location, family composition and caregiver digital skills.

Level of Digitalization and Digital-Use Dynamics

Jordan's Digital Transformation Strategy and Implementation Plan 2026–2028 sets out a framework for secure, inclusive, and sustainable digital transformation. The strategy brings together digital government services, digital infrastructure, privacy and digital trust, digital participation and inclusion, the legislative and regulatory environment, and entrepreneurship and innovation within a common implementation framework (MoDEE, 2026b). Of particular relevance to families is the growing availability of digital public services and records in areas such as civil status, education, health insurance, social security, and family documentation.

SANAD is a central platform in Jordan's digital public-service architecture. It combines digital identity, electronic signatures, a personal document wallet, and single-sign-on access to hundreds of public services. The World Bank documents iterative improvements informed by user feedback (World Bank, 2024b). The 2025 Digital Public Infrastructure Diagnostic provides a roadmap for further developing this infrastructure around trust, interoperability, and inclusion (Tullis, 2025).

Digital public services can make administrative procedures more flexible in terms of time and place. The digitalization of health insurance, social security, civil-status documents, payments, and appointment services can reduce travel and waiting costs, particularly for parents with substantial caregiving responsibilities, older people, and individuals with limited mobility. Jordan also operates digital channels alongside face-to-face Government Service Centers. According to the World Bank's GovTech case study, four centers were operational by the end of 2023, a center was planned for each governorate, and a National Service Registry and multiple feedback channels were developed to incorporate user feedback into service performance (World Bank, 2024b).

Social media and messaging platforms are widely used in Jordan and can support family communication, school-family interaction, sharing religious and cultural content, news exchange, and small-scale commerce. Their prevalence also provides opportunities for public institutions to deliver safe-use messages through channels where families are already present. Campaigns by NCFA, UNICEF, and JRF using digital communication channels illustrate efforts to disseminate safety information and information on available support (Jordan River Foundation, n.d.-a; Jordan River Foundation & UNICEF Jordan, 2021).

The school-based study by Malak, Khalifeh, and Shuhaiber (2017) and the cross-sectional adolescent study by Abdallah and Hamdan-Mansour (2024) examine problematic internet use and associated characteristics in their respective Jordanian samples.

These observational studies can inform school guidance and family support, but cannot establish that internet use causes family difficulties or estimate current prevalence for all Jordanian children or households.

MoDEE's 2025 Digital Inclusion Policy addresses accessibility, affordability, skills, disability-related access needs, geographic location, legal status, and other barriers to meaningful use (MoDEE, 2025a). Its relevance to family governance is that inclusion is considered not solely through connectivity rates but also through accessible interfaces, understandable language, support channels, device and skill adequacy, and non-digital alternatives.

Taken together, these developments suggest that digital access in Jordan is increasingly accompanied by attention to service accessibility, inclusion, and user support. High connectivity provides a foundation for the expansion of services such as SANAD, while the Digital Inclusion Policy and face-to-face service centers seek to address barriers that connectivity alone may not resolve. From a family-governance perspective, this highlights the importance of considering not only access to digital services but also families' ability to use services and obtain support when needed (MoDEE, 2025a, 2026b; World Bank, 2024b; Tullis, 2025).

Key Trends and Policy Developments in Digital Family Governance

The NCFA–UNICEF National Study on Violence Against Children, published in 2021 with data collected from January to October 2019, examined children aged 8–17 and caregivers, with a national sample and separate samples for specific groups. It found that 13.2% of children aged 8–17 in the national sample reported at least one lifetime experience of cyber violence (NCFA & UNICEF Jordan, 2021, pp. 12, 20). This historical, self-reported measure is not a current annual prevalence estimate; findings for specific groups, including children in Syrian refugee camps and children with disabilities, should be interpreted within their respective samples.

Save the Children Jordan's Behind the Screens (2024) used mixed methods with children aged 10–17 and parents to examine digital experiences, risks, and support mechanisms. It complements the earlier violence study by bringing together child and parent perspectives (Save the Children Jordan, 2024). The two studies differ in age coverage, timing, and measures; their findings should therefore be interpreted within their respective scope.

NCFA's 2018 report, Jordanian Family in Jordan, provides earlier evidence on the effects of digitalization on family relationships. In the 2017 field study covering approximately 2,300 families, 70% of surveyed families perceived reduced time together in connection with internet and social-network use, while 67% considered these technologies a participant in childrearing (NCFA, 2018a, p. 123). These adult-reported perceptions provide a historical baseline, not causal evidence or a measure of current family relationships. Updating such family-level evidence could help track changes in family communication, parental mediation, help-seeking, and child well-being.

Al-Shatnawi et al. (2024) examine cyberbullying in a convenience sample of 428 nursing students at three private universities in Jordan, with data collected in 2022. This student sample adds evidence from young adulthood, but its findings cannot be generalized to all university students, younger children, or Jordanian families.

In privacy and data protection, Jordan has developed a legal and institutional framework that combines data-protection legislation with implementation mechanisms. Personal Data Protection Law No. 24/2023 defines data-subject rights, categories of sensitive data, obligations of data controllers, and the institutional oversight structure (MoDEE, 2023a). The Data Protection Council, the relevant directorate, data-protection-officer regulations, and the Data Protection Impact Assessment Guide provide mechanisms for implementing the law across public institutions and private organizations (MoDEE, 2025b).

For children's data, Jordan's existing data-protection infrastructure provides a basis that could support sector-specific guidance for schools, health institutions, social services, and digital public platforms. The Personal Data Protection Law and the Data Protection Impact Assessment Guide provide relevant safeguards for data-subject rights, security, and higher-risk processing (MoDEE, 2023a, 2025b). From the report's value-based perspective, these safeguards are particularly relevant to the principles of Amanah and Adab and Haya, which emphasize responsible stewardship, privacy, and dignity.

With the expansion of digital identity and payment services, Jordan has an opportunity to integrate safe-use awareness more closely into public-service delivery. SANAD provides a unified access point for digital identity, electronic signatures, public services, feedback, and complaint channels (World Bank, 2024a, 2024b; MoDEE, 2026b). Integrating practical digital-safety guidance into digital-service interfaces and face-to-face support channels could further strengthen safe use.

Media and information literacy are another area relevant to family-centered digital governance. Within the report's value framework, Hifz and Sidq are relevant to skills such as source verification, contextual evaluation, recognition of manipulative content, and critical engagement with online information. Communication initiatives by NCFA, UNICEF, and JRF on cyberbullying and online risks also illustrate the potential for addressing children, parents, teachers, and other caregivers through accessible formats (UNICEF Jordan, 2021; Jordan River Foundation, n.d.-a; Jordan River Foundation & UNICEF Jordan, 2021).

Jordan's Artificial Intelligence Strategy and Implementation Plan 2023–2027 addresses the use of AI across areas including health, education, social protection, employment, and public services, while also addressing safe use, risk management, data, and governance (MoDEE, 2023b). For families, the application of AI in areas such as health, education, social protection, and public services makes issues of safety, accountability, human oversight, and data governance particularly relevant.

Key Digital Threats and Their Impacts on Families and Children in Jordan

Bullying, harassment, and exclusion can carry peer conflict into family life, creating distress, withdrawal, and reluctance to disclose harm. The NCFA–UNICEF study documents abusive messages, account theft, fake-account harassment, and unwanted sexual content; these are observed types of harm, not evidence that all children experience them (NCFA & UNICEF Jordan, 2021).

Sexual exploitation, coercion, and extortion require specialist protection and investigative responses, while fraud, impersonation, and account compromise can put household finances and personal information at risk. Privacy breaches may expose children’s images, school or health records, or sensitive family circumstances.

Misinformation and problematic patterns of use can affect trust, study routines, sleep, and family time. The family-level issue is not screen time alone, but whether use displaces care, shared activities, and supportive communication. The 2017 family survey and the observational studies discussed above provide starting points, while their age and design limit conclusions about current prevalence or causality.

Emerging AI risks include fabricated images and voices, identity impersonation, sexualized deepfakes, deceptive or inaccurate generated content, and disclosure of children’s information to AI tools. AI companions may also create inappropriate dependency or unsafe advice. UNICEF’s guidance identifies these as child-rights and safety concerns internationally; it does not establish their prevalence in Jordan (UNICEF Innocenti, 2025).

A life-course perspective is important because children's digital experiences, levels of autonomy, and protection needs change with age and development. Younger children depend more heavily on caregiver guidance and age-appropriate digital environments, while older children and adolescents increasingly encounter risks associated with peer interaction, privacy, independent platform use, exploitation, financial scams, and emerging technologies. Disability, family support, displacement, and digital capability may further shape needs across different stages of childhood.

4.3.2. Regulatory Framework

Jordan's regulatory framework addresses several areas relevant to digital family governance, including digital rights and responsibilities, personal data protection, safeguards for children, trusted digital services, and institutional responsibilities. The following analysis examines how the main regulatory instruments relate to the protection and support of families and children in the digital environment.

National Strategy, Policy Documents, and Legislation

Jordan's Digital Transformation Strategy and Implementation Plan 2026–2028 brings together digital government services, digital infrastructure, privacy and digital trust, digital participation and inclusion, and the legislative and regulatory environment around a vision of a "digitally empowered and secure Jordan" (MoDEE, 2026b). Of particular relevance to families is the strategy's emphasis on user-centered government services and its support for a life-events-based model that groups services around user needs rather than institutional boundaries. This approach has the potential to simplify families' interactions with public services and improve service accessibility and continuity.

Jordan's inclusion framework is relevant to family governance because digital access is shaped by more than connectivity. Accessibility, affordability, digital skills, disability-related access needs, geographic location, household resources, and legal or documentation status can affect whether family members complete digital procedures independently and safely. Hybrid service channels and assisted access can therefore complement digital delivery, particularly for users who face barriers to independent digital access.

Personal Data Protection Law No. 24/2023 defines personal and sensitive data, regulates data-processing principles and data-subject rights, establishes the obligations of controllers and processors, and provides for the establishment of the Personal Data Protection Council and specialized administrative structures (MoDEE, 2023a, n.d.-c). The law entered into force on 17 March 2024 and has subsequently been supported by implementing regulations and institutional arrangements.

For families, the law is particularly relevant to the protection of personal and sensitive data, including health, religious, financial, genetic, and biometric data. Implementation tools related to data protection officers, record-keeping, data disclosure, and impact assessment provide additional mechanisms for managing data-protection responsibilities (MoDEE, 2023a, 2025b).

Children's Rights Law No. 17/2022 provides a national framework addressing the best interests of the child and rights related to protection from violence, education, health, and development (NCFA, 2022). Although the law is not specifically dedicated to online safety, its broader child-protection provisions are relevant to risks that may also arise in digital environments. NCFA's role in monitoring, research, and policy coordination is also relevant to the implementation and development of child- and family-related policies.

For digital policy, these child-rights principles are relevant to considerations such as the best interests of the child, non-discrimination, privacy, access to beneficial information, participation, and evolving capacities. This interpretation complements national law with the UN Committee on the Rights of the Child’s guidance on the digital environment (2021).

Cybercrime Law No. 17/2023 provides investigation and enforcement tools concerning unauthorized access, misuse of accounts and identities, online blackmail, and certain forms of illegal content (Hashemite Kingdom of Jordan, 2023). For family and child safety, these provisions form part of the broader legal environment for addressing certain forms of harm occurring through digital channels.

Jordan's Artificial Intelligence Strategy and Implementation Plan 2023–2027 addresses capacity building, research, the regulatory environment, public-sector applications, data, and risk-related considerations (MoDEE, 2023b). As AI applications expand into areas relevant to families and children, issues such as human oversight, transparency, non-discrimination, and secure data use are increasingly relevant to the broader governance framework.

Taken together, these instruments address several complementary dimensions of digital family governance, including access to digital services, personal data protection, child protection, cybersecurity, and emerging technologies. Their relevance for families depends not only on the scope of individual laws and strategies, but also on how these different regulatory areas interact in practice.

Table 4.20 Jordan's Policy and Legislative Framework Relevant to Digital Family Governance

Policy or law and status	Purpose and family relevance	Implementation and entities	Area for Further Development	Possible Area of Focus
Children's Rights Law No. 17/2022; enacted	Protection, development, best interests, and participation of children	Relevant sectoral authorities; NCFA supports monitoring, research, and policy coordination	Further consideration of child rights in digital services	Child-rights considerations and safe participation in digital services
Personal Data Protection Law No. 24/2023; effective 17 March 2024	Protection of personal and sensitive data and data-subject rights, including data relevant to families and children	Personal Data Protection Council and relevant administrative structures; controllers and processors are responsible for compliance with applicable safeguards	Further attention to child-accessible information and safeguards in relevant services	Higher-risk processing and accessible complaint mechanisms
Cybercrime Law No. 17/2023; enacted	Legal framework addressing specified forms of cybercrime and online harm, including certain risks relevant to children and families	Competent law-enforcement and judicial authorities	Continued coordination between investigation, protection, and support services	Child-sensitive reporting and referral guidance
Jordanian Digital Transformation Strategy and Implementation Plan 2026–2028; published	Secure and inclusive digital transformation and improved access to digital public services	MoDEE in cooperation with relevant public institutions	Further evidence on families' access to and experience of digital services	Family-relevant service accessibility and continuity indicators
Jordanian Digital Inclusion Policy 2025; published	Meaningful and inclusive access to digital technologies and services across population groups	MoDEE in cooperation with relevant government entities and other stakeholders	Further disaggregated evidence on access and use barriers	Accessible and assisted service channels for users facing digital barriers
Jordan Artificial Intelligence Strategy and Implementation Plan 2023–2027; approved	Development and responsible use of AI, including capacity building, research, regulation, and public-sector applications	MoDEE and relevant institutions involved in implementation of the Strategy and its Implementation Plan	Further attention to child- and family-related risks and human oversight	Safeguards for AI applications relevant to children and families

Source: Authors' analysis of NCFA (2022), MoDEE (2023a, 2023b, 2025a, 2026b, n.d.-c), and Hashemite Kingdom of Jordan (2023). Areas for further development and possible areas of focus reflect the authors' analysis and do not constitute additional statutory mandates or nationally agreed priorities.

Regulatory Tools for Digital Platforms and Content

Online platform governance in Jordan involves several complementary regulatory areas, including telecommunications regulation, personal data protection, cybercrime law, consumer rights, and platforms' own safety mechanisms. The Telecommunications Regulatory Commission (TRC) regulates the telecommunications and information-technology sectors, including matters related to service quality and users' interests, while the personal data protection framework establishes requirements for the processing of personal data. Law-enforcement and judicial authorities address illegal acts falling within the relevant legal framework (TRC, n.d.; MoDEE, 2023a; Hashemite Kingdom of Jordan, 2023). Together, these arrangements provide a framework for addressing different types of digital risk through the relevant institutions.The Personal Data Protection Law requires entities processing personal data in Jordan to comply with applicable data-protection requirements, including those relating to lawful processing, data security, and data-subject rights. Its provisions concerning sensitive data and cross-border data transfers are particularly relevant to the protection of privacy. The Data Protection Impact Assessment Guide provides additional guidance for assessing data-protection risks associated with certain processing activities (MoDEE, 2025b).

The Cybercrime Law and the broader child-protection framework address different aspects of the response to online harm, including criminal investigation, protection, support, and referral through the competent authorities and relevant service providers (Hashemite Kingdom of Jordan, 2023; NCFA, 2018b; Jordan River Foundation, n.d.-b). These mechanisms illustrate the complementary roles of law-enforcement processes, reporting and support channels, and social-service referral in responding to online harm.

Legal Framework for Regulatory Oversight and Implementation

Regulatory and service responsibilities are distributed across different institutions. MoDEE leads digital transformation; the Personal Data Protection Council provides oversight under the data-protection law, and the Personal Data Protection Directorate receives and handles data-protection complaints (MoDEE, 2023a, n.d.-d). TRC regulates communications and user interests. NCFA supports policy, evidence, coordination, and monitoring. The Ministry of Social Development, through its social service offices and protection services, undertakes social assessment, case management within its mandate, referrals, and follow-up. The Public Security Directorate's Family and Juvenile Protection Department handles protection reports and investigations within its jurisdiction, including online sexual exploitation (Ministry of Social Development, n.d.; Public Security Directorate, n.d.). JRF's 110 Helpline is a complementary counseling and referral channel, not a substitute for the competent protection authorities (Jordan River Foundation, n.d.-b).

The institutionalization of personal data protection demonstrates Jordan's approach to supporting legislation with practical tools. Processes such as data inventories, data protection officers, recordkeeping, breach management, and Data Protection Impact Assessments support the accountability of public institutions and private organizations (MoDEE, 2025b). These tools are particularly relevant to institutions processing sensitive data, including child health and social-service data.

NCFA's Policies and Guiding Principles for the Prevention of and Response to Violence in Jordan set out a multisectoral framework for case management, referral, and confidentiality (NCFA, 2018b). Within that framework, Ministry of Social Development social service offices and the Family and Juvenile Protection Department retain their respective service and protection responsibilities; NCFA's coordination and technical support do not replace them.

Jordan's published materials identify several sources that can inform service monitoring and provide information on user and family experiences. For SANAD, user feedback is collected through the "At Your Service" platform, social media, and in-app suggestion and complaint channels, while the National Service Registry includes indicators related to service performance, such as waiting times and satisfaction (World Bank, 2024b). The NCFA–UNICEF and Save the Children studies provide additional evidence on children's experiences, awareness, and help-seeking (NCFA & UNICEF Jordan, 2021; Save the Children Jordan, 2024). Taken together, these sources complement technical usage figures with information relevant to user and family experiences.

Preventive Policies: Education and Awareness

In Jordan, preventive efforts include research, awareness-raising, information provision, and access to support and referral mechanisms. Research by NCFA, UNICEF, and other actors provides evidence on patterns of risk and behavior, while awareness materials are disseminated through schools, portals, applications, and community channels. The 110 Helpline provides a counseling and referral channel, alongside the broader protection and social-service mechanisms available through the competent authorities (NCFA & UNICEF Jordan, 2021; Jordan River Foundation & UNICEF Jordan, 2021; NCFA, 2024). Taken together, these elements illustrate an approach to prevention that combines information provision with pathways for seeking assistance.

A distinctive feature of preventive policy is that awareness messages are complemented by concrete support and referral options. UNICEF's cyberbullying guidance recommends that children speak with a trusted adult, teacher, or school counselor and, where necessary, contact the JRF 110 Family and Child Helpline (UNICEF Jordan, 2021). Presenting the campaign and helpline within the same communication is a good practice that links awareness-raising with practical information on where to seek help.

Schools provide an important setting for digital-safety education and school-family communication. Age-appropriate guidance can address areas such as online respect, empathy, privacy, disinformation, artificial intelligence, and digital well-being. Research in the Jordanian context also highlights the importance of parental guidance and communication in supporting children's safe and responsible engagement with digital technologies (Shawareb et al., 2025). The principles of Adab and Haya, Sidq, and Hifz al-Aql provide relevant reference points for linking these issues to families' cultural and moral language.

National studies in Jordan and JRF–UNICEF campaigns highlight the value of considering children not merely as recipients of protection but also as participants whose experiences can inform understanding of the digital environments in which they live (Save the Children Jordan, 2024; Jordan River Foundation & UNICEF Jordan, 2021). Age-appropriate and safeguarded opportunities for child participation can provide useful input into the design of digital-safety initiatives. This experience may also offer relevant lessons for other OIC Member Countries.

Jordan's prevention approach also includes digital resources that complement campaigns with continuous information and parental support. The Children of Jordan portal increases the visibility of children's rights and protection programs; the Early Childhood Portal consolidates information on policies, programs, and indicators; and the Osraty application provides caregivers of children from birth to age five with developmental activities and guidance (NCFA, n.d.-a, n.d.-b, n.d.-c; NCFA, 2024). Families can therefore access institutional information not only when risk emerges, but also across different stages of children's development.

Complementing these digital resources, the Fortify initiative, launched by the Minister of Social Development in April 2026, and related public communication activities provide practical messages for children, parents, and caregivers (Jordan News Agency, 2026). The initiative illustrates the role of public communication in connecting awareness with practical guidance and information on available sources of support.

4.3.3. Institutional Governance Structure

Jordan's institutional architecture combines national policy coordination with distinct sectoral mandates. The digital-economy authorities provide strategic direction for public digital infrastructure and service standards; NCFA contributes to family and child policy, while sector ministries, regulators, protection services, schools, and civil-society organizations perform specialized prevention, service, and intervention functions.

Strategic Coordination and Family Policy

At the strategic level, MoDEE coordinates national digitalization. NCFA is an independent institution established under Law No. 27 of 2001, with a policy and coordination role: it contributes to policy formulation and guidance, research and information resources, partnerships, monitoring and follow-up, and technical support. It is not a direct service provider or a replacement for sectoral implementing authorities (NCFA, n.d.-d, 2024). Within digital family governance, these functions can support the consideration of family and child policy priorities across relevant areas of institutional work.

At the operational level, responsibilities are distributed across social development, education, health, protection and law-enforcement bodies, the telecommunications and data-protection authorities, and organizations such as the Jordan River Foundation. Together, these actors contribute at different stages of prevention, information provision, detection, reporting, referral, support, and follow-up for families and children.

AMAN is an electronic system supporting the handling of violence cases, including documentation, referral, and follow-up among participating institutions. UNICEF reports expansion to four additional governorates and registration of 6,831 new cases in 2025 (UNICEF Jordan, n.d.). Ministry of Social Development social service offices and the Family and Juvenile Protection Department undertake case-management and response functions within their respective mandates, while NCFA supports coordination and technical development. The system illustrates the role of digital tools in supporting documentation, referral, and follow-up within the broader protection framework.

These arrangements, summarized in Table 4.21, highlight the importance of continuity across access, prevention, support, and intervention in responding to the needs of families and children.

Table 4.21 Institutional Architecture of Digital Family Governance in Jordan

Actor	Core Function	Contribution to Families and Children	Partnership, Referral and Accountability
MoDEE	Digital-transformation policy and public-service infrastructure	Secure and user-centered digital services relevant to families	Relevant institutions retain their respective service responsibilities
Personal Data Protection Council and Directorate	Data-protection oversight; complaints and compliance	Rights and safeguards relating to personal-data processing	Controllers implement applicable safeguards; the Directorate handles complaints under the law
NCFA	Independent policy, evidence, coordination, monitoring, and technical support	Family-policy guidance and support to partner institutions	Coordinates partners; does not replace service providers
Ministry of Social Development and social service offices	Social services and case management within mandate	Assessment, referral, follow-up, and social support	Coordinates with protection, health, and other relevant service providers
Public Security Directorate / Family and Juvenile Protection Department	Protection reports and investigations within jurisdiction	Response to violence and online sexual exploitation	Works with social service offices and relevant judicial authorities within its mandate
Ministry of Education	School policy, teacher capacity, and guidance services	Prevention, early identification, and family communication	Coordination with families and relevant protection and support services
Telecommunications Regulatory Commission	Telecommunications regulation and user protection	Service quality and telecommunications complaints	Coordination with relevant authorities where appropriate
JRF 110 Helpline	Counseling, psychosocial support, and referral	A free, confidential help channel alongside official protection channels	Provides counseling and referral to relevant services

Source: Authors' synthesis of MoDEE (2023a, n.d.-d), NCFA (2018b, n.d.-d), Ministry of Social Development (n.d.), Public Security Directorate (n.d.), TRC (n.d.), and Jordan River Foundation (n.d.-b).

Families and children may enter the protection and support system through different channels, including schools, social service offices, competent protection authorities, and complementary help channels. The relevant institutions perform assessment, referral, protection, support, and follow-up functions within their respective mandates. Coordination among these actors can support continuity across the service pathway, while confidentiality and appropriate data protection remain important throughout the process. At the policy level, NCFA contributes through coordination, monitoring, and technical support rather than direct case management.

4.3.4. Implementation Mechanisms and Policy Instruments

The following practices were selected because they address access, trust, prevention, or intervention; have a documented institutional basis; and offer lessons relevant to families. Selection does not constitute a comparative effectiveness ranking. SANAD and service centers address access; data-protection tools address trust; parenting resources and campaigns support prevention; and competent protection agencies, AMAN, and referral channels support intervention. Their relevance to other contexts depends on national mandates, institutional capacities, accessibility, legal safeguards, and local needs rather than on adopting the same technology or model.

SANAD Digital Identity and Public Services Platform

SANAD is the primary digital public infrastructure tool enabling public services in Jordan to be delivered through a single digital identity. The platform combines digital identity, electronic signatures, a personal document wallet, notifications, payments, and access to hundreds of services. The World Bank's SANAD case study documents in detail the transition from institution-centered e-government portals to a user-centered one-stop model and how iterative design increased adoption (World Bank, 2024a).

The platform's family-centered value lies in bringing together, at a single access point, services needed at different stages of life. According to the World Bank case study, by the end of 2023, SANAD had brought together more than 500 digital services, including birth, marriage, divorce, and death certificates; health insurance cards; social security services; payments; and appointment procedures (World Bank, 2024b). By reducing the need for in-person visits, such services can save time and travel costs for working parents, caregivers, older people, and families living in remote areas.

The World Bank's 2024 account also records an improvement in SANAD's app rating from 1.8 to 4.8 following its redesign (World Bank, 2024b). This experience illustrates the importance of user-centered design in improving the accessibility and usability of digital public services. From a family perspective, service-use information and user feedback can provide further insight into how digital services respond to the needs of different users and households.

Personal Data Protection Implementation and Awareness

The implementation of the Personal Data Protection Law is a fundamental condition for families to use digital services with confidence. The law grants data subjects' rights of access, rectification, objection, and, under certain conditions, erasure, while imposing obligations of transparency, security, and accountability on data controllers (MoDEE, 2023a). These rights enable families to question how their health, school, social assistance, biometric, and civil status data are used.

Jordan's strength in data protection lies in its development of implementation tools that translate the law into institutional routine. Data-protection officers, records, disclosure procedures, breach management, and Data Protection Impact Assessments support the identification and management of risks associated with the processing of personal data (MoDEE, 2025b). This approach can also be considered in relation to the governance meaning of Amanah, whereby public and private actors are responsible not only for protecting data but also for explaining what data they use and why, and for correcting errors.

For children and families, these safeguards are particularly relevant to institutions and services that process sensitive information, including schools, health providers, social services, and digital platforms. Clear information on data use, secure handling of records, and accessible mechanisms for exercising data-subject rights can help families understand and use the protections provided under the law. MoDEE identifies the Personal Data Protection Directorate as the recipient of complaints under the law (MoDEE, n.d.-d).

JRF 110 Family and Child Helpline and Case-Referral Network

The 110 Family and Child Helpline, operated by the Jordan River Foundation, provides a complementary channel for families to access counseling, psychosocial support, positive parenting guidance, supportive assessment, and referral to appropriate services (Jordan River Foundation, n.d.-b, n.d.-c). Formal protection reports, case response, and statutory decisions remain with the competent authorities, while the helpline can refer callers to relevant services according to their needs and circumstances.

The distinctive value of the helpline for digital family governance is that it connects online incidents with children's psychological well-being and family support. UNICEF's cyberbullying guidance recommends that children speak to a trusted adult and, where necessary, contact the 110 helpline (UNICEF Jordan, 2021). In this way, in-platform reporting, criminal complaints, and psychosocial support can serve as different intervention pathways depending on the nature of the incident and the support required.

The joint JRF-UNICEF campaign against online exploitation explicitly promoted the 110 line as providing inter-institutional referrals and supporting families with positive parenting practices (Jordan River Foundation & UNICEF Jordan, 2021). Combining a campaign message with a trusted help channel in the same communication is a strong design principle that links awareness-raising with access to support services.

Aggregated and appropriately protected information from helpline and case-management mechanisms can contribute to a better understanding of emerging needs and patterns of harm. Considered alongside research findings, such information can help inform prevention, referral, and family-support efforts (NCFA, 2024; Jordan River Foundation, n.d.-d; NCFA & UNICEF Jordan, 2021).

Children's Digital-Safety Campaigns (NCFA-UNICEF and Partners)

NCFA, UNICEF, JRF, Save the Children Jordan, and other partners conduct research-based awareness activities on cyberbullying and online exploitation. Under JRF's #Mush_Sah campaign, films for children, adolescents, and families, a coloring book, and a training guide for service providers were prepared; translating content into sign language also supported accessibility for children with disabilities (Jordan River Foundation, n.d.-a). This multimodal and accessible communication is a good practice in inclusive campaign design.

One strength of these campaigns is their ability to translate technical safety language into behavioral messages that children and families can understand and apply. These messages encourage children and families to talk to someone they trust, not to share harmful content, to preserve evidence, to report to the platform, to protect their personal information, and to ask for help (UNICEF Jordan, 2021; Jordan River Foundation & UNICEF Jordan, 2021). Connecting these messages with principles of compassion, respect, privacy, and safety brings value-based communication and children's rights together in a single language.

Save the Children Jordan's research, conducted jointly with children and parents, highlights the value of considering the needs and experiences of different target groups in digital-safety initiatives (Save the Children Jordan, 2024). Child-focused content can be complemented by information and guidance for parents, teachers, and caregivers, while age-appropriate and safeguarded child participation can help ensure that communication remains relevant to children's experiences.

In addition to documenting campaign reach and engagement, information on changes in awareness, safe-use practices, and help-seeking can provide further insight into how preventive activities are experienced by children and families. Such information can complement existing evidence on campaign materials, delivery approaches, and participation.

Viewed together, these tools illustrate different but related dimensions of digital family governance in Jordan. Research and service data can help identify needs, while portals, applications, and campaigns contribute to preventive capacity. SANAD and hybrid centers facilitate access to services, and data-protection measures support trust. The helpline and case-management mechanisms provide intervention and referral when harm occurs. Evidence generated through these different mechanisms can also contribute to institutional learning and the continued development of policy and educational approaches. Table 4.22 summarizes the main features of these digital family-governance tools (NCFA, 2024; World Bank, 2024b; Jordan River Foundation, n.d.-c).

Table 4.22 Comparative Analysis of Digital Family-Governance Tools in Jordan

Dimension	SANAD	Data Protection Regime	JRF 110 Helpline	NCFA–UNICEF Campaigns
Primary Focus	Digital public services and identity	Privacy and data-subject rights	Counseling, support, and referral	Prevention and awareness
Target Group	Citizens and progressively expanding user groups	Data subjects; public and private organizations	Children, parents, and families	Children, parents, and educators
Core Strength	One-stop and scalable service delivery	Legal rights and institutional safeguards	Confidential support and referral	Accessible formats and prevention messages
Intended Family Outcome	Reduced time and transaction burden	Protection of family and child data	Access to support following harm	Risk awareness and help-seeking
Area for Further Development	Continued attention to inclusive and user-centered access	Further attention to child-accessible information and awareness	Continued attention to digital risks and service follow-up	Further evidence on outcomes and user experience
Possible Area of Focus	Family experience of digital and assisted service channels	Accessible information on rights and complaint procedures	Effective referral and continuity of support	Awareness, safe-use practices, and help-seeking

Source: Created by the Authors.

NCFA Digital Information, Parenting, and Early Childhood Ecosystem

NCFA's portals and parenting resources support its policy, evidence, and technical-guidance role through accessible information. The Children of Jordan portal makes children's rights, protection programs, and multisectoral partnerships visible; the Early Childhood Portal aims to bring together institutional programs, research, and indicators in a shared information environment (NCFA, n.d.-a, n.d.-b). These tools provide policymakers with access to relevant information and offer reference resources for families and professionals.

The Osraty application provides parents and caregivers with age-organized activities that support the motor, cognitive, linguistic, social, and emotional development of children from birth to age five (NCFA, n.d.-c). Its importance for digital family governance lies in bringing early-childhood policy into families' everyday caregiving practices. From the report's value-based perspective, this can be considered in relation to Hifz al-Usra (Protection of the Family) and Hifz al-Nasl (Protection of Progeny), not only at moments of protective intervention but also through preventive family support that strengthens healthy child development.

The Children of Jordan, the Early Childhood Portal, and the Osraty initiatives illustrate three relevant functions of NCFA's digital tools: making public information more accessible, increasing the visibility of relevant information and programs, and supporting parents in everyday caregiving. The Jordanian experience also highlights the value of digital resources that connect evidence and service information with age-appropriate guidance for parents and caregivers.

Government Service Centers and Hybrid Access

Jordan's digital service model complements the SANAD application with Government Service Centers across the country. According to the World Bank's GovTech case study, four centers were operational by the end of 2023, and centers were planned across the governorates so that citizens and businesses could access services and receive face-to-face support (World Bank, 2024b). The centers assist with digital-identity activation and multi-agency transactions. These dated figures describe the situation reported in 2024, not the current number of centers.

For families, the value of this hybrid approach is that it helps maintain alternatives to exclusively digital service delivery. The World Bank highlights the importance of preserving analog and face-to-face alternatives for reducing the risk of excluding users with limited connectivity or digital skills (World Bank, 2024b). For older people, persons with disabilities, individuals with limited digital skills, and parents and caregivers, this approach highlights the value of combining digital services with human support, accessibility, and continuous user feedback.

Information on the use of in-person support can provide useful insight into the accessibility of digital public services for different groups of users. Continued use of face-to-face channels may indicate that an important alternative is serving its intended purpose, rather than a failure to adopt digital services.

Digital Inclusion Policy and e-Participation

A family-centered approach also requires attention to households that face structural barriers to digital participation, including rural residence, low income, limited digital skills, disability-related access needs, language barriers, displacement, or insecure documentation. The relevant outcome is not identical use across all groups, but safe and meaningful access to essential services with appropriate support and alternatives.

Jordan's e-participation policy and SANAD's "At Your Service," social media, and in-app suggestion and complaint channels position citizens not only as recipients of services but also as participants in service improvement (World Bank, 2024b). For families, these channels provide opportunities to communicate issues related to access, language, trust, and usability to relevant institutions. Continuous user feedback can, in turn, contribute to the accessibility and responsiveness of digital services for different groups of users.

Digital Skills and Families' Economic Resilience: Youth, Technology and Jobs

The Youth, Technology and Jobs programme supports digital skills and income opportunities, including for young people, women, and Syrian refugees (MoDEE, n.d.-a). Although its primary focus extends beyond digital family governance, it is relevant to the extent that digital skills and access to economic opportunities can affect the circumstances in which families engage with digital transformation.

The programme therefore illustrates the broader connection between digital inclusion, skills development, and the economic circumstances of families. The implementation mechanisms discussed above address several dimensions relevant to digital family governance, including access to services, trust in relation to personal data and rights, prevention and family support, and intervention when harm occurs. Table 4.23 summarizes the main practices discussed in this section, their relevance to families and children, and their key features from a digital family governance perspective.

Table 4.23 Selected Practices and Key Features of Digital Family Governance in Jordan

Selected Practice	Lead Actor(s)	Contribution to Families and Children	Key Policy Feature	Transferable Lesson / Area for Further Development
SANAD digital identity and one-stop service	MoDEE	Life-event-based service access; potential time and travel savings	User-centered and life-event-based service design	Attention to families' experience of digital and assisted service channels
Government Service Centers	MoDEE / public institutions	Face-to-face support for users who may require assistance in accessing digital services	Hybrid and accessible service delivery	Combining digital services with accessible face-to-face support
Personal data protection implementation tools	Data Protection Council and Directorate	Rights and safeguards for family, health, education, biometric, and children's data	Implementation tools supporting data-protection requirements, including DPOs, DPIAs, guidance, and complaint mechanisms	Accessible information on rights and safeguards, including for children and families
National Child Studies	NCFA, UNICEF, Save the Children	Evidence on children's experiences and parental awareness	Evidence generation and child participation	Attention to study dates, populations, and scope when interpreting findings
JRF 110 Family and Child Helpline	Jordan River Foundation	Free and confidential counseling, psychosocial support, and referral	Links between awareness, helpline support, and relevant protection and support services	Connecting awareness-raising with accessible support and referral channels
Digital Inclusion Policy and institutional support	MoDEE	Attention to barriers affecting different groups of families and users	Accessibility, meaningful access, and citizen participation	Combining digital access with appropriate support and alternative service channels
Youth, Technology and Jobs	MoDEE / World Bank partnership	Digital skills, employment, and economic participation	Links between digital skills, employment, and economic opportunities	Recognition of the broader relationship between digital inclusion and families' economic circumstances
NCFA digital information and parenting ecosystem	NCFA / UNICEF / Plan International	Children's-rights information, early-childhood information, and age-appropriate parental guidance	Integration of information, evidence, and caregiver support	Connecting policy information and evidence with practical guidance for parents and caregivers
AMAN electronic case management	Ministry of Social Development and social service offices; Family and Juvenile Protection Department; partner providers; NCFA coordination	Case documentation, referral, and follow-up among participating institutions	Mandate-based case management supporting documentation, referral, and follow-up	Supporting continuity across protection and social-service pathways while respecting institutional mandates and confidentiality

Source: Authors' synthesis of the practice-specific sources cited above. The table summarizes documented features and their relevance to families and children; their applicability to other contexts depends on national mandates, institutional capacities, resources, and safeguards.

Overall, Jordan has established important legal, institutional, and digital-service foundations relevant to digital family governance. The experience also points to areas for continued development as technologies, family needs, and digital risks evolve, including up-to-date evidence, accessible and inclusive service delivery, data protection, age-appropriate digital-safety guidance, and attention to emerging AI-related risks.

4.3.5. Lessons Learned

The Jordanian experience illustrates the importance of coordination across the different functions of digital family governance. Access, trust, prevention, and intervention involve different actors, and the case offers lessons that other OIC Member Countries may adapt to their own institutional and social contexts.

1. Strengthen connections across access, trust, prevention, and intervention
Digital public services, data protection, family guidance, reporting, referral, and support create greater value when they are coordinated across relevant institutions and services. Other OIC Member Countries may adapt this lesson by identifying the institutions responsible for different functions and strengthening coordination and referral where these functions intersect.

2. Combine central coordination with clear multi-stakeholder responsibilities and referral protocols
Jordan illustrates that strategic coordination does not require every function to sit in one institution. What matters is a common direction, clear institutional responsibilities, agreed referral procedures, proportionate information sharing, and feedback on case outcomes.

3. Design family services around life events, hybrid access, and privacy
Life-event-based digital services can reduce administrative and caregiving burdens when they are accompanied by face-to-face or assisted alternatives, understandable procedures, secure authorization, data minimization, and effective complaint channels. Success should therefore be assessed not simply by the number of services placed online, but also by whether families can use them effectively and with confidence.

4. Link evidence, family capacity-building, and trusted help channels
Research on children's experiences is most useful when it informs parenting resources, school and community guidance, behavior-oriented communication, helplines, referral, and follow-up. Linking awareness-raising with practical guidance and trusted help channels can provide families with a clearer route from recognizing a problem to obtaining support.

5. Integrate values into policy design
The Islamic value framework provides a complementary perspective alongside national law, the child-rights framework, and relevant international standards; it is not intended as the sole normative basis for digital policy. Principles related to stewardship, responsibility, protection, privacy, dignity, and proportionality can help connect digital governance with the well-being of families and children and with questions of responsibility, protection, and appropriate technology use.

Jordan's experience brings together digital-service infrastructure, a data-protection framework, family-policy coordination, and multisectoral protection mechanisms. These elements illustrate how existing institutions and initiatives can provide a foundation for continued development as family needs, technologies, and digital risks evolve. For other OIC Member Countries, the broader lesson is to build on existing institutional strengths while adapting governance arrangements and safeguards to national circumstances.

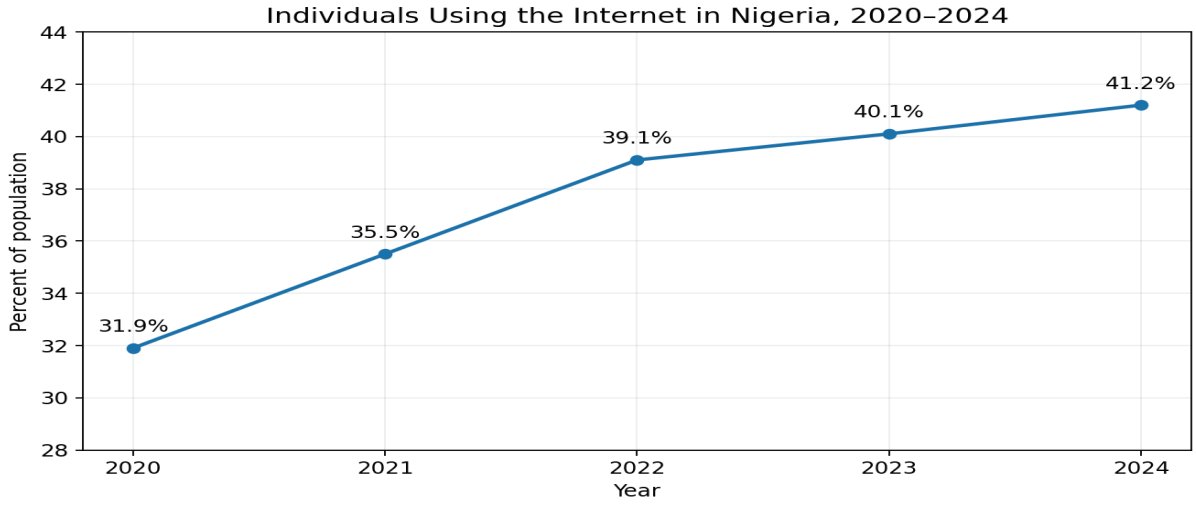
4.4. NIGERIA

4.4.1. Introduction

Nigeria is a federal state composed of 36 states and the Federal Capital Territory and is a member of the Organization of Islamic Cooperation. The United Nations Population Fund estimates the country's 2025 population at 237.5 million. Its very young population structure, mobile-first digitalization, and differences in access and capacity across states make online safety relevant not only as a technology-policy issue but also as a matter of family well-being, children's rights, and inclusive development. The principal feature that makes Nigeria relevant to this report is the need to deliver digital policy instruments to a large, young, and socially diverse population (UNFPA, 2025).

A distinctive feature of the Nigerian case is its multi-actor approach, which brings together communications regulation, data protection, cybersecurity, children's rights, digital literacy, parental guidance, and specialized reporting mechanisms through different institutions. When the 2026 Internet Code of Practice, Nigeria Data Protection Act, NITDA's National Digital Literacy Framework, and Digital Literacy for All (DL4ALL) program, the Nigerian Communications Commission's multilingual child-safety materials, and ACSAI's helpline linked to the INHOPE network are considered together, an emerging multi-actor model of digital family governance can be identified. The purpose of the analysis is not to list these instruments, but to explain their complementarity, implementation conditions, and transferable functions for other OIC Member Countries.

Figure 4.8 Individuals Using the Internet in Nigeria, 2020–2024



Source: World Bank World Development Indicators, based on ITU data

Family Structure and Social Values

Family arrangements in Nigeria display a plural structure in which extended-family solidarity and nuclear-household practices coexist. Grandparents, adult siblings, aunts, and uncles may assist with childcare, educational expenses, housing, and support during crises. Internal and international migration can reduce the physical proximity of these networks, while digital platforms provide new means for sustaining kinship relations. Messaging groups, video calls, and mobile money transfers can extend family solidarity beyond geographic boundaries.

This community-oriented family context provides an important foundation for digital child protection. Digital-safety awareness and guidance can therefore benefit from engaging not only parents but also extended family members involved in caregiving, as well as teachers and relevant community actors. Such an approach recognizes the different relationships through which children may receive guidance and support.

Family authority and respect for elders remain important norms in many communities, while children's experiences in digital environments may differ considerably from those of adults. Children may be more technically skilled in using certain digital tools, but technical familiarity does not necessarily equip them to recognize online manipulation, fraud, harmful interactions, or risks to personal data. Similarly, parents and caregivers may benefit from practical guidance on platform settings, privacy options, and reporting tools. Effective digital parenting therefore requires technical skills and value-based judgment to be treated as complementary rather than alternative capacities.

Academic studies in Nigeria provide further insight into family communication and parental mediation. Egielewa and Umolu (2022) examined the effect of smartphone use on family communication and indicated that intensive use may weaken face-to-face communication. Adigwe and van der Walt (2020) examined how parents regulate children's online-media activities from a parent-child perspective. Their findings show that restrictive, active, monitoring, and co-learning strategies can be used together within the same family.

These findings suggest that the duration of technology use is only one dimension to consider and highlight the relevance of communication, family guidance, parental digital literacy, and children's age-appropriate autonomy.

Nigeria's extended-family and community networks may also support the implementation of digital-safety initiatives. Parents, other family members involved in caregiving, teachers, and relevant community actors can play complementary roles in prevention, guidance, early identification, and referral. Community-based and locally accessible approaches can help connect national digital-safety initiatives with the social networks through which families receive information, guidance, and support.

Level of Digitalization and Digital-Use Dynamics

Nigeria's digitalization is large-scale but varies across regions and population groups. Mobile connectivity is the primary form of internet access, particularly given the challenges associated with extending fixed infrastructure across a large territory. For families, smartphones can provide access to educational content, public information, mobile banking, and communication through a single device. At the same time, effective and safe use can be influenced by factors such as data affordability, device availability, electricity supply, and mobile network quality. Where devices are shared among family members, additional considerations may also arise regarding children's personal accounts and privacy.

Meaningful digital participation also varies across Nigerian households. Income, education, age, disability-related access needs, rural residence, access to reliable electricity, device quality, data costs, and digital skills can all shape how family members access and benefit from digital services. These differences highlight the importance of considering household-level conditions alongside national connectivity indicators (World Bank, 2025b).

For children and young people, smartphones can bring learning, entertainment, peer communication, content creation, and economic opportunities together within a single interface. This multifunctionality means that opportunities and risks may coexist within the same digital environments. For example, an application used for an online lesson may also provide access to age-inappropriate content, while social networks used for communication may expose children to interactions beyond their immediate social circles. Child-safety policy therefore needs to consider design features, data practices, age safeguards, and reporting mechanisms across different types of digital services and platforms.

Nigeria's digital-economy policy recognizes digital skills as a core component of economic transformation. The National Digital Economy Policy and Strategy 2020–2030 identifies eight key pillars, including infrastructure, regulation, digital literacy, indigenous content, and digital services. Through NITDA's 2024–2027 Strategic Roadmap, the National Digital Literacy Framework, and the Digital Literacy for All initiative, a target of 70% digital literacy by 2027 has been established. From a digital family-governance perspective, these broader digital-literacy efforts also provide opportunities to strengthen parents' and caregivers' awareness of online risks, communication with children, access to support, and use of available safety tools (Federal Ministry of Communications and Digital Economy, 2020; NITDA, 2023, 2024).

For digital family governance, national connectivity and digital-literacy indicators can therefore be considered alongside household-level access, digital skills, privacy awareness, safe-use practices, and access to appropriate guidance and support.

Table 4.24 Key Demographic and Digital Indicators for Nigeria

Indicator	Value	Year / Source	Relevance to Digital Family Governance
Population	237.5 million	2025, UNFPA	Scale of child- and family-oriented policy delivery
Population aged 0–14	Approximately 41%	2025, UNFPA	Importance of child online protection
Internet users	Approximately 107 million (45.4%)	Early 2025, DataReportal	Scale and reach of digital participation
Social media user identities	Approximately 38.7 million (16.4%)	Early 2025, DataReportal	Scale of social media use
Individuals using the Internet	41.2%	2024, World Bank/ITU	Internationally comparable measure of internet use
Digital literacy target	70% by 2027	NITDA SRAP 2.0 / DL4ALL	Potential reach of nationwide digital-literacy initiatives

Source: UNFPA, 2025; Data Reportal, 2025; World Bank/ITU, 2024; NITDA SRAP 2.0.

Key Trends and Risk Areas

Evidence from academic research and relevant institutional sources identifies a number of recurring areas of online risk for children and families in Nigeria. The analysis below focuses on these documented risk areas while taking into account the scope and coverage of the available evidence.

Evidence from Nigerian households indicates that online risks and parental responses are heterogeneous rather than uniform (Adigwe, 2024). Different risks—including fraud, cyberbullying, privacy concerns, harmful contact, misinformation, and excessive use—may require different combinations of family guidance, shared rules, technical tools, and referral support. This highlights the importance of risk-specific and developmentally appropriate approaches to digital safety.

These risks also underline the importance of ensuring that children and young people know how to respond when they encounter problems online. Technical measures such as blocking and reporting tools are important, but they need to be complemented by family guidance and accessible sources of support. Open communication within the family can help children seek assistance when problems occur and enable parents and caregivers to respond appropriately to different types of digital risk (International Telecommunication Union [ITU], 2020).

Online sexual exploitation of children and child sexual abuse material represent particularly serious forms of online harm. In this context, Nigeria joined the international hotline network through the Action Against Child Sexual Abuse Initiative (ACSAI) in 2024. This development provides a specialized mechanism for reporting illegal material and supporting cooperation at the international level.

Cyber fraud, phishing, and account takeover can also affect families' economic security. While mobile banking and fintech applications facilitate access to financial services, the same communication channels may also be misused for fraudulent activities, including social engineering and identity theft. Children and adults may encounter different forms of online fraud, highlighting the relevance of practical cybersecurity awareness within families. Such guidance can extend beyond password security to include verification of suspicious requests, awareness of fraudulent messages, and appropriate reporting procedures.

Disinformation and inaccurate information can also affect family decision-making. Information shared through messaging groups may circulate through existing networks of family and community trust, underscoring the importance of digital and media literacy. In this context, the ability to assess the source, evidence, date, and reliability of online information is an important component of informed digital participation.

Privacy risks may arise both from the sharing of children's personal information and images and from data-processing practices in digital environments. The Nigeria Data Protection Act includes provisions concerning the processing of children's personal data, including parental or guardian consent requirements. In the context of "sharenting," considerations such as the child's age, the sensitivity of the information or image, location information, school identity, and potential longer-term implications highlight the importance of protecting children's privacy in family digital practices.

Finally, AI-supported chat, content-generation, and recommendation systems represent an emerging area of both opportunity and risk. AI can support education, language translation, and access to information, while also raising concerns related to misinformation, biased outputs, personal-data disclosure, and age-inappropriate content. As AI-enabled services continue to evolve, child online-safety frameworks may increasingly need to consider issues such as age-appropriate design, data protection, transparency, and developmental appropriateness.

These risk areas highlight the importance of a balanced approach that enables children to benefit from digital opportunities while strengthening appropriate safeguards. Such an approach can combine service-provider responsibilities for safer digital environments and accessible reporting, open communication within families, school- and community-based digital and media literacy, protection of children's data, specialized reporting and support mechanisms, and appropriate referral where necessary. This distributes responsibility across families, public institutions, service providers, and other relevant actors rather than placing the burden of digital safety primarily on children or parents.

4.4.2. Regulatory Framework

Nigeria's regulatory framework is formed by the intersection of instruments concerning children's rights, cybercrime, data protection, communications services, national cybersecurity, and digital literacy. This multilayered structure provides legal bases and specialized institutional capacity for addressing different types of digital risks. From a family perspective, an important consideration is how these instruments work together to provide accessible pathways from risk prevention and reporting to investigation and appropriate support.

National Strategy, Policy Documents, and Legislation

The National Digital Economy Policy and Strategy 2020–2030 (NDEPS) provides a key framework for Nigeria's digital-transformation agenda. The document brings together core pillars including digital literacy and skills, digital infrastructure, service infrastructure, digital services development, indigenous content, and digital society. From a digital family-governance perspective, the framework is relevant because it addresses digital skills alongside the broader infrastructure and services needed for digital participation (Federal Ministry of Communications and Digital Economy, 2020).

The Child Rights Act 2003 provides a fundamental rights framework concerning the best interests, development, privacy, and protection of children from exploitation. Although the online harms children face today were not anticipated in their current forms when the law was adopted, its provisions concerning exploitation, abuse, inhuman treatment, and privacy provide relevant principles for addressing harms that may also occur in digital environments (Federal Republic of Nigeria, 2003; UNICEF Nigeria, 2025).

The Cybercrimes Act 2015, as amended in 2024, provides the principal federal legal framework concerning offenses committed through computer systems and includes provisions addressing child sexual abuse material. Together with the broader child-protection and data-protection framework, it contributes to Nigeria's legal response to serious forms of online harm (Federal Republic of Nigeria, 2015, 2024).

The Nigeria Data Protection Act 2023 established a comprehensive framework for the processing of personal data and created the Nigeria Data Protection Commission (NDPC). Section 31 addresses the processing of children's data, including parental or legal guardian consent where consent is relied upon as the lawful basis for processing, as well as age- and consent-verification requirements. The NDPC's 2025 General Application and Implementation Directive provides further operational guidance (Federal Republic of Nigeria, 2023; NDPC, 2025). The Act also provides specified exceptions to the parental-consent requirement.

The National Cybersecurity Policy and Strategy 2021 provides a high-level framework for cyber-incident preparedness, critical infrastructure, awareness, cooperation, and capacity building. Although families are not its primary target group, the strategy contributes to the broader national framework for addressing cyber risks that can also affect households, including fraud, identity theft, and malware (Office of the National Security Adviser, 2021).

Regulatory Tools for Digital Platforms and Content

The Internet Code of Practice 2026 extends the regulatory framework to areas including platform governance and online child protection. Its provisions concerning safeguards, parental-control measures, and safety tools complement the guidance and supervision that families can provide at home and recognize a role for service providers in protecting children online. The accompanying Guidance Notes on the Internet Code of Practice 2026 clarify regulatory expectations and implementation arrangements, including those relating to online child protection (NCC, 2026b).

Technical safeguards are most effective when complemented by parental guidance, digital literacy, and accessible reporting mechanisms. In this respect, the Code can be considered alongside broader educational and family-support measures rather than as a stand-alone mechanism for managing children's online risks.

NCC research on children's use of digital technologies also highlights issues relating to children's online privacy and age-appropriate protection. These findings reinforce the relevance of continuing to develop child-sensitive safeguards as digital services and patterns of use evolve (NCC, 2024a).

Legal Framework for Regulatory Oversight and Implementation

Regulatory oversight in Nigeria has a multi-actor structure. The NCC operates in communications and internet services; the NDPC in personal-data processing; the Office of the National Security Adviser and ngCERT in cyber-incident coordination; law-enforcement agencies in the investigation of cybercrime; and social-service and child-protection institutions in victim support. This distribution enables different institutions to contribute specialized functions within the broader digital-protection framework.

The Child Online Access Protection Bill (HB 244) represents an effort to develop a legal framework specifically dedicated to children's online safety. The Bill passed the House of Representatives in December 2025 and received its first reading in the Senate on 7 July 2026. As of September 2026, it remains within the legislative process and should therefore be distinguished from the legal framework currently in force.

The Bill is relevant because it reflects continuing legislative attention to online child safety as a distinct policy area. Its consideration also provides an opportunity to address issues such as institutional responsibilities, child-friendly complaint and confidentiality safeguards, children's participation, and mechanisms for monitoring implementation as the legislative process continues.

Legal Integration of Preventive Policies (Education and Awareness)

In Nigeria's policy framework, digital literacy increasingly encompasses dimensions of digital safety and citizenship alongside economic and technical skills. NITDA's National Digital Literacy Framework includes information and data literacy, communication and collaboration, digital content creation, safety, and problem-solving. The Digital Literacy for All (DL4ALL) initiative aims to extend basic digital skills across the country's 774 local government areas. This nationwide delivery structure also provides opportunities for integrating family-oriented digital-safety and awareness content (NITDA, 2023, 2024).

The 3 Million Technical Talent (3MTT) program complements broader digital-literacy initiatives through its focus on technical skills and employability. While it is not primarily a child- or family-protection program, it forms part of Nigeria's wider efforts to strengthen digital capabilities among young people (Federal Ministry of Communications, Innovation and Digital Economy, 2026).

The NCC's Keeping Children Safe Online materials and Parenting 101 for Digital Citizens activities provide practical guidance for parents and caregivers. These initiatives complement regulatory measures by bringing online-safety awareness into everyday family settings (NCC, 2024b, 2025). NCC's public resources confirm both sets of materials.

These preventive instruments illustrate how digital-safety considerations can be combined with broader digital-literacy initiatives and parental guidance. Their reach can be further supported through accessible formats, including local-language materials and content adapted to different connectivity and accessibility needs.

4.4.3. Institutional Governance Structure

Nigeria's institutional architecture brings together specialized institutions operating across federal, state, and local levels. The Ministry provides strategic direction; the NCC establishes service-provider obligations and user-protection measures; the NDPC safeguards data rights; NITDA supports digital skills and capacity development; ONSA/ngCERT coordinates responses to cyber incidents; law-enforcement and child-protection institutions provide investigative and victim-support functions; and ACSAI operates a specialized reporting hotline. This institutional structure brings together specialized functions while highlighting the importance of clear and accessible coordination and referral pathways for families.

Macro and Strategic Level (Ministries and Coordinating Bodies)
The Federal Ministry of Communications, Innovation, and Digital Economy is responsible for the strategic coordination of national digital policy, innovation, infrastructure, and digital-economy programs. NDEPS, 3MTT, and the digital public-infrastructure agenda are shaped at this level. From a digital family-governance perspective, the Ministry's broader digital-policy mandate provides an important entry point for integrating considerations related to inclusion and digital safety.

The Office of the National Security Adviser is a high-level actor responsible for cybersecurity coordination under the National Cybersecurity Policy and Strategy. Cyber-incident response and warning functions are carried out through ngCERT. These functions are also relevant to cyber risks affecting households, including fraud and malware.

Operational and Technical Level (Specialized Agencies)
NITDA plays an important operational role in digital literacy, technology capacity, standards, and digital transformation. Through initiatives such as the National Digital Literacy Framework (NDLF) and DL4ALL, it supports digital-skills development at scale. From a digital family-governance perspective, this delivery capacity also provides opportunities to integrate relevant digital-safety and awareness content into broader digital-literacy efforts.

The Nigeria Data Protection Commission is the national data-protection authority established under the Nigeria Data Protection Act (NDPA) 2023. It is responsible for overseeing the implementation of the Act, promoting the protection of personal data, issuing guidance, monitoring compliance, and handling relevant complaints.

Regulatory and Implementation Level
The Nigerian Communications Commission occupies a central position as the economic, technical, and consumer-focused regulator of telecommunications and internet services. The Internet Code of Practice, online child-protection materials, and parental-awareness activities make the NCC an important actor in digital family governance. Its regulatory and consumer-protection functions complement the roles performed by institutions responsible for areas such as data protection, cybersecurity, law enforcement, education, and social services.

The Action Against Child Sexual Abuse Initiative (ACSAI) operates the Nigerian hotline that joined the INHOPE network in 2024. INHOPE's 2024 Annual Report states that the service operates in cooperation with the Nigeria Police and child-protection stakeholders. The hotline provides a specialized mechanism for reporting online child sexual abuse material and facilitating appropriate referral and cooperation.

Within this multi-actor institutional structure, effective coordination and referral mechanisms are particularly important for connecting reporting, assessment, platform or hotline referral, law-enforcement and social-service support where necessary, and feedback to children and families. Clear functional pathways can help families understand the respective roles of different institutions and support coordination across levels of government.

4.4.4. Implementation Mechanisms and Policy Instruments

Nigeria's approach brings together four complementary implementation channels:

- obligations for service providers and data processors;
- preventive capacity building for children, parents, teachers, and community actors;
- reporting mechanisms for illegal or harmful content; and
- referral to relevant legal, technical, and psychosocial support.

Although these functions are distributed across different institutions, together they illustrate a broader protection, empowerment, and response framework.

Nigerian Communications Commission Child Online Protection Program and Multilingual Localization

The Nigerian Communications Commission's Child Online Protection activities comprise materials, research, and awareness initiatives that adapt the ITU's child online protection approach to the Nigerian context. The Commission provides online-safety guides for children, parents, and educators in digital formats. The Keeping Children Safe Online document emphasizes open communication with children, awareness of privacy settings, discussion of children's online interactions, and support when harm occurs.

The availability of resources in widely used Nigerian languages, including Hausa, Yoruba, Igbo, and Nigerian Pidgin, broadens the accessibility of child online-safety guidance across different linguistic communities. Publishing multilingual versions of Agent COP materials also illustrates how linguistic accessibility can be incorporated into the delivery of digital-safety information rather than treated solely as a subsequent translation exercise. This approach highlights the relevance of adapting communication channels and formats to the linguistic and accessibility needs of different communities (NCC, 2026).

NITDA Digital Literacy and DL4ALL

The National Digital Literacy Framework and Digital Literacy for All (DL4ALL) initiative are relevant to digital family governance because their broad delivery structure provides an existing channel through which digital-safety awareness can complement wider digital-skills development. Areas such as privacy, online fraud, misinformation, source verification, and safe digital practices are particularly relevant to the family-centered perspective of this report (NITDA, 2023, 2024).

From this perspective, the relevance of these initiatives extends beyond participation targets to the practical digital capabilities they seek to strengthen. For families, such capabilities may include safer account and data practices, source verification, awareness of online risks, and knowledge of available support and reporting mechanisms. This illustrates the potential connection between national digital-skills policies and broader family-centered digital governance.

ACSAI-INHOPE Child Sexual Abuse Material Reporting Hotline
The ACSAI-INHOPE mechanism provides a specialized reporting channel for online child sexual abuse material and facilitates cooperation across relevant national and international actors (INHOPE, 2025). Its role is particularly relevant for serious forms of online harm that require specialized handling beyond ordinary customer-service or platform-reporting channels.

The mechanism also illustrates the importance of connecting specialized reporting with appropriate referral and response arrangements. More broadly, such mechanisms demonstrate the relevance of confidential and child-sensitive reporting pathways capable of supporting cooperation across platforms and jurisdictions.

Parenting, School, and Community-Based Safety Tools
NCC activities such as Parenting 101 for Digital Citizens frame parents' role in children's online lives not simply in terms of restrictions, but also through communication, shared learning, and role modeling. Adigwe's (2021) study with 1,270 parents in Lagos found that parental digital literacy was particularly associated with co-learning. The findings highlight the relevance of approaches in which parental guidance and children's evolving digital knowledge can complement one another.
Such approaches place emphasis on communication and a

ge-appropriate guidance alongside technical supervision. They may include listening to children's experiences, explaining the reasons behind family rules, discussing privacy boundaries, and creating an environment in which children can seek support when needed. Schools, extended-family members involved in caregiving, and relevant community actors can also complement parents' role in promoting digital safety and help-seeking.

4.4.5. Lessons Learned

Nigeria's experience illustrates how national digital-safety and digital-literacy frameworks can be supported through local, linguistic, educational, and community-based channels across a large and diverse population. The lessons below focus on the broader implementation functions illustrated by the case rather than on individual program names.

1. **Combine National Frameworks with Locally Accessible Implementation**

Nigeria's experience highlights the relevance of combining national frameworks with implementation through different levels of government, schools, communities, and other relevant actors. Clear institutional responsibilities and referral pathways can help connect these different levels while allowing implementation to respond to local contexts.

2. **Make Family-Oriented Digital and Media Literacy Accessible and Context-Sensitive**

The use of local languages and different communication channels illustrates the importance of adapting digital-safety guidance to the contexts in which families access information. Schools, community-based channels, extended-family members involved in caregiving, and other relevant actors can complement national digital-literacy initiatives and help extend family-oriented guidance beyond online campaigns alone.

3. **Combine Family Guidance with Service-Provider Responsibilities**

Families play an important role in communication, role modeling, shared rules, and children's help-seeking. At the same time, service-provider responsibilities relating to child protection, privacy, parental tools, user information, and reporting mechanisms provide complementary safeguards within the wider digital environment. Nigeria's regulatory and awareness-raising measures illustrate the importance of addressing both dimensions together.

4. **Link Specialized Reporting with Appropriate Referral and Response**

Serious forms of online harm require specialized and child-sensitive reporting mechanisms that can facilitate cooperation with relevant platforms, law-enforcement authorities, child-protection services, and international networks where appropriate. The ACSAI-INHOPE mechanism illustrates the value of connecting specialized reporting with broader referral and response arrangements rather than relying solely on general platform or customer-service channels.

These lessons illustrate the value of combining national frameworks with locally accessible implementation, family-oriented capacity building, service-provider responsibilities, and specialized reporting and referral mechanisms. For other OIC Member Countries, these functions may provide useful reference points while allowing institutional arrangements and delivery mechanisms to be adapted to national and local contexts.

Viewed through the value framework of this report, the Nigerian case is particularly relevant to Hifz (protection of the family, progeny, and intellect) and Mas'uliyyah (responsibility). Measures aimed at protecting children and families from digital risks can be considered in relation to Hifz, while the complementary roles of families, public institutions, service providers, and other relevant actors are consistent with the principle of Mas'uliyyah. These linkages provide an analytical lens for considering the Nigerian case within the report's broader value framework, rather than implying that the policies examined were explicitly designed on the basis of these principles.

4.5. HUNGARY

4.5.1. Introduction

Hungary is subject to European Union regulations on data protection, audiovisual media, and digital services, while also giving family and child-rearing a prominent place at the constitutional and public policy levels. A distinctive feature of the case is the presence of regulatory, research, low-threshold reporting, media literacy, parental guidance, and digital public service mechanisms that perform complementary functions in relation to children and families. Hungary, therefore, provides a useful comparative case for examining how these different functions interact within a broader digital governance environment affecting families and children.

The case is particularly relevant for examining the combination of National Media and Infocommunications Authority's (NMHH) regulatory responsibilities with research, media literacy, and the Internet Hotline; the relationship between platform responsibilities under the EU Digital Services Act and national reporting mechanisms; and the use of the Digital Citizenship Programme (DÁP) to facilitate access to public services through life-event-based digital services (NMHH, 2024a, 2026d; Digital Citizenship Programme, 2026).

As a non-OIC reference case, Hungary is examined within its own regulatory and institutional context, while the report's value-based analytical framework is applied selectively to consider the implications of relevant policies and practices for families and children.

Family Structure and Social Values

Article L of Hungary's Fundamental Law protects marriage and the family as the basis of the nation's survival and states that commitment to having and raising children shall be supported. This constitutional framework helps explain the central position of family policy (Government of Hungary, 2011/2026).

Data from the Hungarian Central Statistical Office show long-term demographic changes in population and fertility. The population stood at approximately 9.54 million as of 1 January 2025. The total fertility rate was 1.45 in 2015 and 1.59 in 2020, then declined to 1.39 in 2024 and to 1.31 in the preliminary data for 2025 (Hungarian Central Statistical Office, 2025, 2026).

According to findings publicly reported in 2025 by the Mária Kopp Institute for Demography and Families, 98% of respondents in Hungary regarded family as very important, compared with 88% in the European sample. The average ideal number of children in Hungary was also reported as 2.4. These findings provide additional context for understanding the prominence of family-related issues in Hungarian public and social life. (KINCS, 2025a, 2025b).

Digitalization increasingly affects multiple dimensions of family life, including communication, school-family relations, health, administrative procedures, care coordination, and kinship ties. Research in the Central and Eastern European context, including Hungary, shows that while video calling, messaging, and social-media tools help sustain contact among geographically dispersed family members, generations differ in platform preferences, messaging habits, and privacy expectations (Deák et al., 2024). Digital technology does not automatically strengthen family ties, nor does it automatically weaken them. Its effects vary according to how technology use is embedded in family routines and relational rules (Bărbuță et al., 2023).

This social context highlights the importance of considering the family not only as an institution to be protected, but also as an important actor at the intersection of digital services and online risks. This strong family orientation can be complemented by parents' capacity for guidance, children's participation, equitable access to services, and institutional mechanisms supporting safe digital practices.

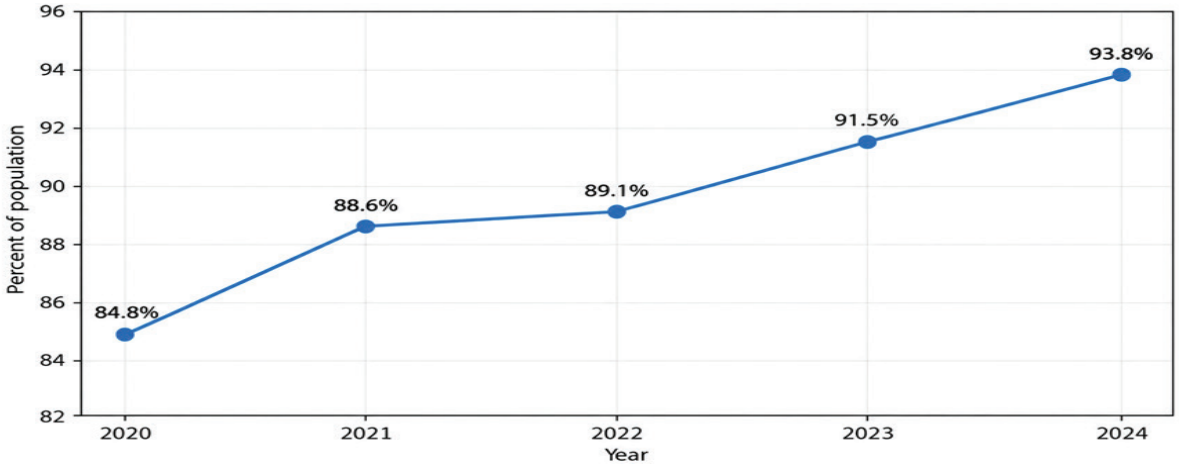
Level of Digitalization and Digital-Use Dynamics

According to DataReportal's 2025 country overview, Hungary had approximately 9.05 million internet users, with internet penetration at 94.1%. The number of active mobile connections reached approximately 11 million, and the number of social media user identities approximately 6.84 million. These indicators point to the widespread integration of digital communication and platform use into everyday life (DataReportal, 2025). As shown in Figure 4.9, the share of individuals using the internet also remained high over the 2020–2024 period.

The European Commission's 2026 Digital Decade assessment also highlights Hungary's fiber infrastructure and digital public services for citizens (European Commission, 2026).

Hungary's high level of connectivity does not eliminate differences in meaningful use. Household resources, age, digital skills, disability-related access needs, and local service conditions can still affect independent access to digital services and support. This highlights the continuing relevance of accessible, multichannel assistance even in highly connected digital environments.

Figure 4.9 Individuals Using the Internet in Hungary, 2020–2024



Source: World Bank World Development Indicators, based on ITU data

Key Trends and Risk Areas

Children are entering digital life at increasingly younger ages. NMHH research from 2017, 2020, and 2024–2025 indicates that children aged 7–16 are using phones and social media at increasingly younger ages. A representative study published in 2021 reported that the proportion of 7–8-year-olds owning a phone had risen from 14% to 24% within three years, that most 10-year-olds had a mobile phone, and that the proportion of 11–16-year-olds contacted by strangers online had increased from 9% to 18%. The same study found that approximately one-third of parents did not regularly use any of the approaches of prohibiting, limiting, monitoring, or discussing children's online experiences (NMHH, 2021).

A study published in 2026 involving 1,875 parents showed that digital device use was widespread among children aged 3–6. It reported that approximately 9 out of 10 preschool children used a digital device, 71% of parents viewed the effects of screen time on development as predominantly negative, and 83% of children who used devices had difficulty stopping their use. Children's average weekly screen time was 7.7 hours (NMHH, 2026f).

Another academic study of Hungarian families found that parenting strategies were significantly associated with children's mobile-device use. Research by Konok, Bunford, and Miklósi with 1,283 parents showed that parents' own device use, approaches to rule-setting, and communication with the child jointly shaped children's patterns of use. This finding highlights the relevance of parental role modeling, explanatory guidance, and age-appropriate shared rule-setting alongside approaches based primarily on prohibitive control (Konok et al., 2020).

Reports to Hungary's Internet Hotline reflect a range of online harms, including online sexual abuse, non-consensual content sharing, phishing, online bullying, and AI-generated intimate content. The Internet Hotline received 2,575 reports in 2025, approximately 80% of which required action. Online child sexual abuse accounted for 32% of all reports (NMHH, 2026d).

In the European Commission's 2026 public opinion indicators, 94% of respondents supported stronger online protection for children and young people, and the same proportion identified online privacy and security as priorities for the coming decade (European Commission, 2026).

These findings highlight the importance of shared responsibility across families, schools, platforms, regulatory authorities, helplines, and social-support actors in addressing children's digital risks. This includes combining age-appropriate information and digital competence with accessible reporting and support mechanisms. Table 4.25 summarizes the key findings discussed above and their relevance to digital family governance.

Table 4.25 Selected Findings on Families and Digitalization in Hungary

Indicator / Finding	Reported Finding / Value	Source	Relevance to Digital Family Governance
Population	Approximately 9.54 million (1 January 2025)	Hungarian Central Statistical Office	Provides the demographic context for family-policy and digital-service planning
Total fertility rate	1.59 (2020); 1.39 (2024); provisional 1.31 (2025)	Hungarian Central Statistical Office	Provides demographic context for the prominence of family- and child-related policy issues
Internet use	Approximately 9.05 million users; 94.1%	DataReportal 2025	Indicates the broad reach of digital services and online environments
Social media user identities	Approximately 6.84 million	DataReportal 2025	Shows the relevance of platform governance and family media literacy
Pre-school digital-device use	Around nine in ten children use a digital device	NMHH 2026	Highlights the relevance of digital guidance from early childhood
Digital-parenting research	Repeated waves in 2017, 2020 and 2024–2025	NMHH	Provides evidence for tracking changes in children's digital use and parental practices over time

Source: Hungarian Central Statistical Office; DataReportal, 2025; NMHH, 2026.

4.5.2. Regulatory Framework

Hungary's regulatory framework brings together layered constitutional family and child protection, data protection, media and communications law, criminal law, national strategies, and directly applicable EU regulations. These layers address complementary aspects of prevention, platform accountability, reporting, referral, and trust in digital services.

Constitutional and General Child-Rights Framework

The Fundamental Law provides the general framework for the protection of the family and child-rearing. Children's personality rights, private life, and image are addressed under civil law and child-protection provisions. Halász's examination of Hungarian law notes that children's rights in the digital age are addressed at the intersection of constitutional law, child-protection law, data protection, and media legislation (Halász, 2025).

The European Union's General Data Protection Regulation recognizes that children's personal data requires special protection and establishes principles of transparency, legal basis, data minimization, and accountability for online services (European Union, 2016; Halász, 2025).

Digital Child Protection Strategy and Preventive Policy Approach

Hungary's Digital Child Protection Strategy (Digitális Gyermekvédelmi Stratégia - DGYS) was adopted by Government Decision No. 1488/2016 (IX.2). The Strategy's primary objective is to protect children from dangerous and harmful online content and practices while preparing children, parents, and teachers to use the internet consciously and productively. The document is important in that it seeks to balance protection and empowerment. Rather than focusing solely on content blocking, it adopts a multidimensional approach that includes media literacy, education, awareness-raising, research, assistance, and inter-institutional cooperation (Government of Hungary, 2016; Better Internet for Kids, 2024).

A notable feature of the DGYS is that it approaches digital child protection not merely as a technical cybersecurity issue but also as a pedagogical, legal, and social matter. It also emphasizes cooperation among public education, civil society, the child-protection system, and law-enforcement authorities.

The Digital Education Strategy is part of a broader educational transformation aimed at developing digital competencies in schools. From the perspective of digital family governance, its relevance lies in complementing the role of parents through the development of children's digital competencies within the education system.

EU Digital Services Act and National Implementation

The Digital Services Act (DSA) establishes an EU-wide framework for online intermediary services covering areas such as reporting illegal content, transparency, child protection, risk assessment, and platform accountability. In Hungary, the President of the National Media and Infocommunications Authority (NMHH) has been designated as the Digital Services Coordinator. This role includes receiving user complaints, cooperating with institutions at national and EU levels, certifying trusted flaggers, and supervising intermediary service providers established in the country. Primary oversight authority for very large online platforms and search engines remains with the European Commission (European Union, 2022; NMHH, 2025a).

For families and children, an important contribution of the DSA is its emphasis on platform responsibilities concerning risks associated with online services, including transparency, reporting, and child protection. The fact that complaints concerning very large platforms were referred to the coordinators of the relevant countries, as reported in NMHH's 2024 coordinator report, illustrates the role of cross-border cooperation in the implementation of the DSA (NMHH, 2025a).

The Internet Hotline's acquisition of "trusted flagger" status under the DSA as of 25 October 2024 created a stronger link between the hotline and platform processes. Notifications submitted by trusted flaggers must be processed by platforms with priority and without undue delay. This status does not, however, turn the hotline into a court or an administrative enforcement authority. Legal and institutional responsibility for decisions to remove content remains subject to the procedures of the relevant service provider and competent authorities (NMHH, 2026b).

Suppression of Internet Aggression and Criminal Law

Act LXXVIII on the Suppression of Internet Aggression, adopted on 17 December 2024 and entering into force on 1 January 2025, amended existing legislation to restrict aggression in the online environment and introduced a criminal-law provision concerning internet aggression into the Criminal Code. The regulation targets certain publicly accessible content on electronic communications networks that promotes violent acts or expresses an intent to commit them. Non-consensual image sharing, violations of personality rights, data protection, and other matters remain subject to other criminal-law provisions (Better Internet for Kids, 2025a, 2025b).

Hungary has progressively developed obligations for internet service providers to offer protective filtering solutions for minors. Since 1 January 2026, safe mobile internet services for minors have been available through Magyar Telekom, One Hungary, and Yettel Hungary.

Individual subscribers may request the service free of charge. For fixed-line providers, implementation is being extended in phases during 2026 and 2027, based on subscriber numbers (NMHH, 2025b).

Digital State and DÁP

Act CIII of 2023 on the Digital State introduced rules for delivering digital public services in a user-centered, life-event-based manner. The Digital Citizenship Programme (DÁP) aims to integrate public services into a single, easy-to-use digital environment. The application provides functions such as authentication, access to public and certain private services, viewing and sharing personal and vehicle data, digital signatures, an official inbox, and appointment booking at government service centers (Government of Hungary, 2023; Digital Citizenship Programme, 2026).

Although DÁP is not directly a child-protection program, it is a digital governance instrument that affects families' administrative lives. Because life events such as birth, care, health, education, and social support involve multiple institutions, a trusted digital identity and single-point access can reduce the time and transaction costs borne by families.

This regulatory architecture has three complementary functions. The DGYS and media literacy tools aim to prevent harm and promote competence. The DSA, data protection rules, and criminal law aim to hold platforms and data processors accountable. The DÁP supports secure digital identities and user-centered access to services. This regulatory architecture therefore addresses protection and digital participation as complementary rather than opposing objectives. Their contribution to families and children is also shaped by accessibility, coordination, and implementation in practice.

Table 4.26 summarizes the main regulatory and policy instruments discussed above and their relevance to families, children, and digital family governance.

Table 4.26 Regulatory and Policy Framework for Digital Family Governance in Hungary

Instrument	Core Function	Contribution to Families and Children	Relevance to Digital Family Governance
Fundamental Law	Constitutional protection of family and child-rearing	Provides a high-level value and policy mandate	Links digital-governance considerations to the broader family-policy framework
Digital Child Protection Strategy (2016)	Education, awareness, research, protection, and cooperation	Balances protection with empowerment of children, parents, and educators	Brings regulation, literacy, assistance, research, and cooperation within a common strategic framework
GDPR	Data protection and accountability	Special protection for children's personal data	Provides privacy and data-protection safeguards relevant to digital services used by children and families
Digital Services Act	Platform accountability, transparency, and complaint mechanisms	Provides mechanisms for systemic risk management and child protection	Links national oversight and reporting mechanisms with cross-border platform governance
Act LXXVIII of 2024	Addresses defined forms of online aggression	Provides a criminal-law response to specified forms of publicly expressed or promoted violence online	Adds a specific legal instrument addressing defined forms of online aggression
Filtered Internet Service (from 2026)	Optional protective filtering for minors	Free technical protection offered through operators	Adds an accessible technical protection option for minors alongside other child-safety measures
Digital State Act / DÁP	User-centered digital identity and public services	Facilitates access to digital public services relevant to families' administrative needs	Connects secure digital identity and life-event-based public-service delivery with families' access to services

Source: Created by Authors.

4.5.3. Institutional Governance Structure

Strategic Family Policy and Evidence Generation

Digital family governance in Hungary is not concentrated within a single ministry. Responsibilities are distributed among government units responsible for family policy, culture, and innovation; education and child-protection actors; digital-state organizations; the media and communications regulator; law-enforcement bodies; helplines; and civil society. This structure brings together different areas of expertise.
Within this distributed structure, different institutions perform complementary functions in research, regulation and oversight, preventive education, reporting and referral, and psychosocial support. These functions can be illustrated as follows:

1. Research provides evidence on risks and parental behaviors.
2. Regulatory authorities provide standards and oversight.
3. Preventive initiatives such as Magic Valley, Gyerekaneten.hu, and Net-Coach support media literacy and preventive capacity.
4. The Internet Hotline provides a reporting channel and, where relevant, facilitates referral to platforms or competent authorities.
5. Civil-society services such as Kék Vonal provide psychosocial support.

In this way, different institutions and services can address the legal, pedagogical, and psychosocial dimensions of digital risks through their respective mandates.

The Mária Kopp Institute for Demography and Families (KINCS) was established by the Government of Hungary in 2018 and is mandated to conduct research and analysis, and to develop policy recommendations in the fields of family policy and demography. Its institutionalized research capacity is important for supporting the family-policy agenda with evidence. KINCS describes itself as a publicly funded think tank (KINCS, 2025b).

An important component of evidence generation in the digital family field is the NMHH's repeated research on children's and parents' media use. The 2017, 2020, and 2024–2025 waves make it possible to observe change over time. These studies cover not only duration of use but also policy-relevant indicators such as parental concerns, mediation strategies, use of technical controls, children's risk experiences, and awareness of assistance services.

NMHH and the Media Council: Where Regulation and Prevention Converge

The National Media and Infocommunications Authority (NMHH) is the national regulatory authority for electronic communications and media. The Media Council operates within the NMHH as an independent regulatory body responsible for media services. A distinctive feature of the institution's role in digital family governance is that, alongside conventional oversight functions, it also conducts media literacy activities, research, parental guidance, and assistance services.

The President of the NMHH also serves as Hungary's Digital Services Coordinator under the DSA. This role brings together complaint handling, supervision, cooperation with trusted flaggers, and EU-level coordination within the national digital services ecosystem. This arrangement places online-platform oversight and relevant child-protection functions within the same institutional setting.

The Media Council is responsible for promoting media literacy and coordinating the work of different state actors in this field. Magic Valley centres, Gyerekaneten.hu, Net-Coach, and activities for families are instruments of this preventive role. These activities illustrate how regulatory functions are complemented by preventive and educational measures (NMHH, 2024a, 2024b, 2026c).

Internet Hotline: Reporting, Legal Assistance, and Referral

The Internet Hotline is a free legal-assistance and reporting service operated by the Office of the NMHH since 2011. Children and adults can submit reports at any time without providing their names or contact details. The service accepts reports in categories including non-consensual dissemination of content, online child sexual abuse material, online harassment, racist content, or content inciting hatred against a community, content promoting the use of illegal psychoactive substances, incitement to violence or unlawful conduct, phishing, and other content harmful to minors (NMHH, 2026b).

The Internet Hotline does not conduct administrative-authority investigations, cannot compel the removal of content, and cannot impose fines. Experts assess reports, contact content or hosting providers when appropriate, explain the available options to the reporting person, and refer cases involving suspected criminal offenses to the competent investigative authorities. The use of child-friendly language in its communication with children and referral to helplines such as Kék Vonal when psychological support is needed illustrate how legal and psychosocial support can be differentiated yet connected.

The Internet Hotline's trusted-flagger status under the DSA means that its notices are to be processed by platforms with priority and without undue delay. In 2025, 32 percent of reports received concerned online child sexual abuse, 18 percent involved non-consensual content sharing, and 17 percent concerned phishing. The Hotline served as a trusted flagger in 828 cases; service providers acted following notification in 688 cases, and 55 percent of responses were provided within 1 to 3 days (NMHH, 2026d).

Education and Media-Literacy Institutions

The NMHH established the Bűvösvölgy (Magic Valley) media-literacy centers to provide free, experiential education for students aged 9–16. At the three centers in Budapest, Debrecen, and Sopron, students experience content production processes and develop critical-thinking skills regarding news, advertising, social media, and online opportunities and risks. The program extends media literacy beyond classroom-based learning by enabling children to experience the role of content producer (NMHH, 2024a).

Gyerekaneten.hu is an information portal operated by the NMHH to help parents, caregivers, and educators understand children's digital world and manage risks. Rather than merely presenting a list of dangers, the portal encourages parents to talk with children about their online experiences, which is consistent with an active-mediation approach. In the 2024–2025 study, awareness of the portal increased from 23 percent in 2020 to 36 percent, while awareness of the Internet Hotline rose from 19 percent to 27 percent (NMHH, 2024b, 2026e).

The Net-Coach adult education and professional community program aims to train specialists who can help young people and families understand digital media. Its 2023 launch, through cooperation between the NMHH and Apor Vilmos Catholic College, complements online information resources by developing a network of trained intermediaries who can support young people and families. This intermediary-based approach also highlights the relevance of consistent information and referral pathways across professionals working with children and families (NMHH, 2023).

Civil Society and the Support Network

Hungary's Safer Internet Center is a multi-stakeholder structure under the EU's Better Internet for Kids program that brings together awareness-raising, helpline, and illegal/harmful content reporting functions. The 116 111 helpline, operated by the Kék Vonal Child Crisis Foundation, is available nationwide, free of charge, anonymously, and 24 hours a day, and also offers online chat and email counseling (Better Internet for Kids, 2026).

Within this institutional structure, the NMHH combines regulatory functions with research, education, and reporting mechanisms, while civil-society actors provide complementary support services. Where digital harms intersect with family relationships, school safety, and social-service needs, coordination and referral across these different actors can support continuity between reporting, guidance, and psychosocial assistance.

Table 4.27 summarizes the main actors and mechanisms discussed above and their respective roles in Hungary's digital family governance structure.

Table 4.27 Institutional Architecture of Digital Family Governance in Hungary

Actor / Mechanism	Core Role	Contribution to Families and Children	Relevance to Digital Family Governance
Family-policy institutions and KINCS	Family research and policy analysis	Provides demographic and family-related evidence	Adds an institutional evidence-generation function to the broader family-policy framework
NMHH and Media Council	Media, communications, and digital-service regulation	Combines regulation with research, literacy, and prevention	Brings regulatory, research, media-literacy, and preventive functions within the same institutional setting
Digital Services Coordinator	National DSA coordination and cross-border cooperation	Handles complaints and links national actors to EU processes	Connects national oversight and complaint mechanisms with cross-border digital-services governance
Internet Hotline	Anonymous reporting, legal guidance, and referral	Connects users to platforms, authorities, and psychosocial help	Provides a low-threshold reporting and assistance mechanism with links to relevant services and authorities
Magic Valley	Experiential media-literacy education	Allows children to learn by producing and analyzing media	Adds an experiential dimension to preventive media-literacy education
Gyerekaneten.hu and Net-Coach	Parent guidance and professional capacity building	Supports active mediation through online and local intermediaries	Combines online parental guidance with professional capacity building
Kék Vonal / Safer Internet Centre	Child helpline, awareness, and counseling	Provides free, anonymous, and continuous support	Complements reporting and awareness mechanisms with child-centered psychosocial support
DÁP	Digital identity and integrated public services	Facilitates families' interaction with public administration	Links integrated digital public services with families' access to administrative services

Source: Created by Authors.

4.5.4. Implementation Mechanisms and Policy Instruments

Hungary uses a range of implementation tools addressing different aspects of digital family governance. Parental guidance and media-literacy initiatives support preventive capacity, while filtered internet services provide a technical protection option for minors. The Internet Hotline provides reporting, legal guidance, and referral mechanisms, and DÁP facilitates access to digital public services. Initiatives addressing artificial intelligence and child influencers reflect attention to emerging issues affecting children and families. These instruments illustrate how preventive, protective, reporting, support, and service-access functions are addressed through different but complementary mechanisms.

From Reporting to Intervention: Internet Hotline Implementation Chain

The Internet Hotline's operating logic forms a four-stage chain from reporting to intervention. In the first stage, a child or adult submits a free and anonymous report through an online form. In the second, experts assess the nature and accessibility of the content, where it is hosted, and its possible legal category. In the third stage, when necessary, a notice is sent to the content or hosting provider; cases involving suspected criminal offenses are referred to law enforcement or the competent investigative authority.

In the final stage, the reporting person is informed of the available options and, where psychosocial needs are identified, is referred to an appropriate support service.

This process connects a low-threshold, free reporting mechanism with platform and law-enforcement processes. Anonymous reporting and child-friendly explanations can make reporting and the available options more accessible to children. Trusted-flagger status under the DSA provides for priority processing of the Hotline's notices by platforms. In 2025, service providers acted following notification in 688 cases, providing an indication of the operational use of this reporting mechanism (NMHH, 2026d).

Active Parental Mediation

The NMHH's 2024–2025 Digital Parenting study classifies the strategies used by families as restriction, monitoring, active mediation, and technical limitation. Fifty-seven percent of families use rules or prohibitions, 58 percent use monitoring, 47 percent use active mediation, and 53 percent use technical solutions. Compared with 2020, restrictions and personal monitoring have decreased while the use of technical tools has increased. A notable finding is that only about one-fifth of rules are developed jointly with children's participation, and that rules also apply to parents in only about one-third of families (NMHH, 2026e).

The findings indicate that joint rule-setting and parental role modeling remain less common than some other forms of parental mediation.

Magic Valley, School Programs, and Scalable Media Literacy

The Magic Valley program makes critical thinking tangible by allowing children to experience how media messages are produced. Observing selection, framing, and editing processes in a news studio, analyzing advertising's persuasive strategies, and discussing the logic of social media content production and distribution provide an experiential approach to media literacy. This approach moves beyond information-based awareness-raising by engaging children directly with the processes through which media content is produced and interpreted. Net-Coach and Gyerekaneten.hu provide complementary forms of support: Net-Coach provides professional adult education, while Gyerekaneten.hu offers an online information and guidance channel for parents, caregivers, and educators (NMHH, 2024a).

Filtered Internet Service for Minors

The filtered internet service introduced on mobile networks in 2026 provides free technical protection as part of the basic subscription. Activation on request allows adult users to retain freedom of choice while enabling parents to use the service on a child's line. The service is being extended to fixed-line providers in phases during 2026 and 2027, according to provider size (NMHH, 2025b).

DÁP and Families' Access to Digital Public Services

DÁP provides integrated access to a range of digital public-service functions, including mobile authentication, a data wallet, digital signatures, an official inbox, and appointment booking. By bringing these functions together within a single digital environment, the program is designed to simplify users' interactions with public administration and reduce repetitive authentication and document-processing requirements. For families, this model is particularly relevant to administrative procedures that intersect with work, caregiving, and other family responsibilities (Digital Citizenship Program, 2026).

Emerging Risks: Artificial Intelligence, Synthetic Content, and the Child-Influencer Economy

Hungary's existing tools face new challenges in the era of generative artificial intelligence. AI-generated fake images, "nudifying" applications, voice imitation, personalized scams, and manipulation through chatbots can combine content, contact, privacy, and psychological risks within a single case. The Internet Hotline's 2026 warnings concerning AI-assisted non-consensual nudification applications illustrate how established reporting and protection mechanisms are encountering new forms of digitally facilitated harm.

The child-influencer and "kidfluencer" economy raises new questions about the boundary between family life and commercial activity. A child's everyday life can become revenue-generating content on a parent-managed account. When the parent is both the legal representative and the economic beneficiary, conflicts of interest may arise concerning the child's privacy, working conditions, right to income, and future right to request removal of the content. NMHH's 2026 research communication highlights these risks through the concept of "branded childhood" (NMHH, 2026g).

4.5.5. Lessons Learned

The Hungarian case illustrates a range of complementary functions relevant to digital family governance, including regulation, evidence generation, prevention, media literacy, reporting, referral, psychosocial support, and digital public services. The lessons below draw on these functions to identify transferable design considerations rather than suggesting replication of particular Hungarian institutions.

1. **Connect protection, empowerment, reporting, and support mechanisms**

Regulatory and platform-related safeguards can be complemented by media literacy, parental guidance, accessible reporting, psychosocial support, and follow-up. For OIC Member Countries, the broader lesson is to consider how prevention, reporting, referral, support, and remedy functions can be connected through clearly defined responsibilities and procedures. Where several actors are involved, continuity also depends on appropriate information sharing and referral arrangements that avoid requiring children and families to recount the same incident repeatedly.

2. **Keep institutional mandates clear while connecting child-friendly reporting to platform and support processes**

The Internet Hotline illustrates how clear mandate boundaries can coexist with referral across different services. Accessible and, where appropriate, anonymous reporting can be linked to platforms, law enforcement, legal guidance, and psychosocial support, while clear referral procedures and feedback mechanisms can help maintain continuity across these functions. Such an arrangement allows different actors to contribute according to their respective mandates without requiring a single institution to perform every function.

3. **Combine technical safeguards with family-based media literacy and early-childhood guidance**

Technical filtering can address some forms of exposure, while manipulation, cyberbullying, harmful contact, commercial persuasion, and AI-generated misinformation also require critical thinking and family dialogue. Magic Valley, parental resources, and evidence on early-childhood device use point to a life-course approach that combines age-appropriate technical tools with experiential media literacy, parental role modeling, parent-child dialogue, shared rule-setting, and help-seeking skills (NMHH, 2026d, 2026f). Technical safeguards are therefore most useful as part of a broader approach that supports families' capacity to guide children's digital engagement rather than as a substitute for parental mediation.

4. **Make digital public services family-centered, secure, and genuinely multichannel**

Life-event-based digital services can reduce administrative burdens when they are accompanied by accessible alternatives, secure authorization, data minimization, understandable procedures, assisted support where needed, and age-appropriate safeguards for children's data. A family-centered approach therefore requires attention not only to the availability of digital services but also to whether different household groups, including users with limited digital skills or accessibility needs, can complete essential procedures safely and effectively. Maintaining appropriate assisted or non-digital channels can help ensure that digitalization does not itself become a barrier to essential services.

5. **Support Policy Development through Regular Evidence Generation**

Repeated studies of parental mediation and children's digital experiences provide a useful basis for understanding changes over time and informing policy development. The Hungarian experience illustrates the value of complementing administrative and participation data with evidence on children's and families' experiences, digital practices, and emerging risks. For other OIC Member Countries, the broader lesson is the value of regular evidence generation adapted to national circumstances.

6. **Ensure that governance mechanisms can respond to emerging digital risks**

Generative AI, synthetic and manipulated content, and the growing commercialization of children's online presence illustrate how digital risks can evolve faster than established policy categories. Existing reporting, guidance, and protection mechanisms therefore need sufficient flexibility to address new forms of harm without requiring an entirely separate institutional response to each technological development. This includes attention to AI-generated and manipulated content, biometric and personal data, long-term digital footprints, and potential conflicts between children's interests and the commercial use of their online presence. For OIC Member Countries, the broader lesson is to build adaptive capacity into existing governance mechanisms while keeping the best interests of the child, accountability, and access to remedy at the center.

In conclusion, the Hungarian case illustrates how regulatory, preventive, educational, reporting, support, and digital-service functions can complement one another within a broader governance environment affecting families and children. Its relevance for other contexts lies less in reproducing particular institutions than in considering how these functions can be connected, evaluated, and adapted to changing digital risks.

5. CONCLUSION AND POLICY RECOMMENDATIONS

Family remains a fundamental institution for individual well-being and intergenerational continuity, while also contributing to broader social and economic development through care, the development of human capabilities, value transmission, and participation in social and economic life. The analysis shows that the value of digitalization for families cannot be assessed by connectivity or the number of digital services alone. What also matters is whether digital environments support family well-being and children's development and learning, strengthen families' capacity to adapt to change, and enable safe, meaningful, and appropriately supported participation.

Across the country cases, a common finding is that prevention, protection, support, and remedy work best when they are connected. Early identification, reporting, referral, psychosocial and legal support, recovery, monitoring, and policy learning all have a role to play. Countries may organize these functions differently across ministries, regulators, service providers, schools, civil society organizations, and public platforms. What matters is that families can access the protection and support they need without facing gaps between different institutions and services.

A second common finding concerns shared responsibility. Families remain indispensable because parental mediation, role modeling, open communication, shared learning, and intergenerational value transmission cannot be replaced by regulation. At the same time, the country cases show that families are better able to fulfil these responsibilities when they are supported by safer platform design, understandable rules, school and community capacity-building, accessible public services, specialist reporting mechanisms, and effective remedies. Digital policies can also help families make better use of the opportunities offered by technology. Public institutions, private-sector actors, civil society, and creative industries can contribute by providing safe, age-appropriate, accessible, and culturally relevant digital content and services that support parenting, learning, skills development, family communication, caregiving, and meaningful intergenerational engagement. This also recognizes that actors with greater technical, institutional, or commercial power have responsibilities that go beyond those of individual families.

The comparative analysis also shows the importance of looking beyond activity and service-volume indicators when measuring progress. User numbers, participation in training, reports, downloads, and content-removal figures provide useful information about the reach of policies and services, but they do not show whether families are safer, more capable, or better supported. Monitoring can therefore also consider outcomes such as parent-child communication, family media and AI literacy, confidence in seeking help, privacy practices, meaningful and independent service use, the quality of complaint resolution, repeated harm, user trust, and family and child well-being. Continued monitoring is particularly important as generative AI, synthetic media, biometric systems, algorithmic recommendations, and new commercial practices continue to change the digital environment.

For the wider OIC context, the comparative evidence suggests that cooperation can focus on common needs while allowing Member Countries to develop approaches suited to their own national circumstances. Countries need not adopt identical laws, institutions, or programs. Cooperation at the international level can support common assessment tools, comparable outcome indicators, multilingual family-safety resources, the sharing and adaptation of high-quality family-oriented digital content and services, specialist training, peer learning, hotline interoperability, and structured engagement with global technology companies. Overall, the findings point to the need to move beyond a primary focus on connectivity towards safe, meaningful, inclusive, and value-aligned digital participation; to connect prevention, protection, and support more effectively; to share responsibility among families and other relevant actors; and to place greater emphasis on measurable outcomes for families and children.

These findings provide the basis for the policy recommendations that follow. The recommendations take a family-centered approach, bringing together digital opportunities with protection, support, responsibility, and accountability. They also recognize the wider contribution of families to human development and social and economic development. Drawing on the analysis and country cases, the recommendations are intended to provide practical options that Member Countries can adapt to their own circumstances rather than a single model to be applied across the OIC.

The policy recommendations are grounded in the report's value framework, bringing together the core normative values with the cross-cutting principles of Hikmah and Mas'uliyyah. Together, these principles provide a common basis for family-centered digital policies while allowing Member Countries to adapt specific measures to their institutional, legal, social, and cultural contexts.

On this basis, the policy recommendations are organized around nine mutually reinforcing priorities. A roadmap at the end of the section provides further guidance for their implementation.

1. **Integrate a Family-Centered and Value-Based Approach into Digital Policies**

Digital policies that affect children and families need to consider not only technical and economic outcomes, but also their effects on family and child well-being and longer-term development. This applies to areas such as legislation, platform regulation, artificial intelligence systems, digital identity, e-government services, educational technologies, health platforms, data-sharing arrangements, and public communication. A family-centered perspective brings attention to whether policies and services support safe and meaningful participation while protecting family relationships, children's rights and development, privacy, dignity, and access to effective remedy.

A family-centered approach does not require a choice between protection and participation. Excessive restriction may limit children's access to education, information, creativity, and social participation, while insufficient safeguards may expose them to manipulation, exploitation, privacy violations, or harmful contact. The level and type of risk, children's evolving capacities, and the context of use provide a basis for determining appropriate safeguards. At the same time, responsibility cannot rest solely with families. Parents cannot independently address unsafe default settings, recommendation systems that may expose children to harmful content, exploitative data practices, or ineffective platform reporting mechanisms.

The report's value framework provides guidance in addressing these issues. Amanah and Mas'uliyyah emphasize responsibility for data, safety, and foreseeable risks; Hifz draws attention to the protection of family relationships and children's development; Haya and Adab emphasize privacy, dignity, and respectful interaction; and Sidq highlights transparency and information integrity. Wasatiyyah and Hikmah further emphasize balance, sound judgement, and attention to age, risk, and context. Together, these principles provide a common basis for the design and review of digital policies and services, while allowing Member Countries to adapt their approaches to their own circumstances.

In applying this approach, particular attention is given to the effects of digital policies and services on family relationships, children's rights and development, privacy, participation, and access, as well as to how responsibility is shared among families, public institutions, and service providers. Where appropriate, policy development and review processes can also include age-appropriate consultation with children and meaningful engagement with families, helping ensure that policies and services reflect their experiences and needs.

A family-centered approach also involves enabling families to benefit from digital transformation. Policies can promote digital tools, content, and services that strengthen family communication, support parenting and caregiving, facilitate access to education, health, and family services, and enable meaningful intergenerational engagement. Public institutions, civil society, and private-sector actors also have a role in expanding the availability of safe, age-appropriate, accessible, and culturally relevant digital resources for families. In this way, digital policy can both protect families from digital risks and help them benefit from the opportunities offered by technology, while also supporting their wider contribution to social and economic development.

2. **Strengthen Child and Family Protection and Accountability in Digital Governance**

Effective digital governance requires strong protection and accountability mechanisms for children and families, adapted to national legal and institutional contexts. The analysis across OIC Member Countries points to several common challenges, including fragmented responsibilities, limited attention to families in digital regulation, uneven enforcement, insufficient support for families, and difficulties in keeping national frameworks responsive to rapidly changing global platforms. Addressing these challenges requires greater coordination across legal, regulatory, and institutional frameworks. Responsibility also needs to be shared among public authorities, platforms, service providers, families, and users, rather than placing the burden of managing digital risks primarily on parents and children.

- **Child and family impact assessment:** New or substantially revised digital policies and high-risk services may be assessed for their possible effects on children and families. Relevant considerations include privacy and data use, children's developmental needs, effects on family relationships, different effects on groups of children and families, manipulative or addictive design, and access to appeal and remedy. Such assessments help bring children's best interests and rights into the early stages of policy and service design and place appropriate responsibility on service providers to identify and address foreseeable risks (Committee on the Rights of the Child, 2021; OECD, 2024).

- **Safety- and privacy-by-design**: Platforms and digital service providers need to incorporate privacy and safety protections for child users from the outset. This includes safe default settings, limited data collection, clear and age-appropriate information, restrictions on exploitative profiling and targeted advertising directed at children, and accessible mechanisms for reporting, blocking, and appeal. Parental-control tools complement these measures and active parental guidance rather than replacing the responsibilities of service providers.

- **Proportionate age assurance**: Where age assurance is necessary for protection, the method used needs to reflect the level of risk while avoiding unnecessary collection of identity or biometric data. A single identity-verification model is unlikely to be appropriate for every service. The aim is to establish age where necessary while protecting privacy, participation, and personal data.

- **Accountable artificial intelligence:** AI systems used in education, health, social assistance, counseling, child protection, and other services that significantly affect children and families require appropriate human oversight, transparency, and mechanisms for correcting errors and appealing decisions. Decisions with significant consequences for a child need human involvement rather than relying solely on automated outputs. Independent evaluation of system performance, bias, data sources, and different effects on groups of children provides an additional safeguard (UNICEF Innocenti, 2025).

- **Coherent complaint and remedy mechanisms:** Rules and procedures relating to child rights, personal data, cybercrime, consumer protection, media, and telecommunications need to work together effectively. Families cannot be expected to know in advance which regulator or public authority is responsible for a complex digital incident. A single point of entry or connected complaint system provides a clearer route for families and allows cases to be directed to the appropriate authority while maintaining clear institutional responsibilities and rights of appeal.

3. Strengthen Institutional Coordination for Digital Family Governance

The country cases highlight the importance of coordination among institutions responsible for digital policy, family and child protection, education, data governance, regulation, reporting, and support services. Effective coordination does not require bringing all these responsibilities under a single institution. Different institutions can retain their respective roles, provided that responsibilities, referral procedures, information-sharing arrangements, and lines of accountability are clearly defined.

A permanent coordination mechanism can help bring these different areas together while leaving specific responsibilities with the institutions best placed to carry them out. Its scope may include prevention, digital services, platform oversight, child protection, data governance, education, reporting, referral, support, remedy, and monitoring. Clearly identifying the lead and supporting institutions for these areas, together with referral routes, information needs, timeframes, and follow-up responsibilities, can help identify gaps and reduce uncertainty for families seeking support.

Where several institutions or services are involved in the same family or child protection issue, common definitions and clear referral procedures can reduce duplication and prevent cases from falling between institutions. Secure case-management systems may also support coordination, provided that access to information is limited to what is necessary and that privacy and confidentiality are protected.

Regular evidence on family digital practices, children's online experiences, access to services, reporting outcomes, and parents' digital capabilities can further support institutional coordination and policy development. This function can be carried out by an existing statistical, regulatory, academic, or policy institution rather than requiring the creation of a new body. Linking these findings to the regular review of policies and services can help ensure that emerging needs and implementation gaps are identified over time.

4. **Strengthen Family Capacity Across the Life Course**

A family-based approach to media and AI literacy can connect guidance within the family with schools, family services, health and early-childhood settings, and community-based support. Rather than relying mainly on one-time awareness campaigns, families need access to age-appropriate guidance that responds to their needs at different stages of life. Strengthening media and AI literacy also helps families benefit from digital opportunities for learning, skills development, access to services, and participation in social and economic life.

Support can begin with guidance for parents and caregivers in early childhood and continue through the school years with age-appropriate parent-child activities. For adolescents, relevant areas include privacy, peer interaction, commercial influence, misinformation, and AI, while adults and older family members may require continued support as technologies and digital risks change. The aim is to strengthen communication, shared learning, and problem solving within families rather than placing technical responsibility on parents alone.

Key areas include shared rule-setting, role modeling, source verification, synthetic-media and AI literacy, privacy and data practices, fraud and commercial manipulation, balanced use, respectful communication, and clear routes for reporting problems and seeking help. Local-language, low-data, offline, school-based, community-based, and other locally appropriate forms of delivery can help reach families that may not be well served by online resources alone.

Progress can be assessed through changes in parent-child communication, confidence in discussing digital problems, shared rule-setting, critical evaluation of information, privacy practices, knowledge of available support, and willingness to seek help. This provides a clearer picture of whether initiatives are strengthening families over time rather than simply reaching large numbers of participants.

Family capacity also depends on the digital environment and the resources available to families. Expanding safe, age-appropriate, educational, and culturally relevant digital content and services gives children and families more positive choices. Governments can support the development of family-oriented digital products and content through partnerships with technology developers, creative industries, social enterprises, and other relevant actors, as well as through appropriate support for innovation and the sharing of good practices. These efforts need to be accompanied by appropriate safeguards for child safety, privacy, commercial practices, and content quality.

5. **Make Digital Inclusion and Public Services Family-Centered**

Digital inclusion policies need to take the different circumstances of families into account. Rural residence, low income, limited digital skills, disability-related access needs, language barriers, caregiving responsibilities, displacement, or lack of appropriate devices may affect a household's ability to access and use digital services safely and independently. Essential family-facing services can address these differences through multichannel support, assisted access, accessible design, low-data options, and clear and understandable information.

Digital public services can also be organized around important family life events rather than institutional boundaries. Procedures related to birth, schooling, disability, health, social assistance, civil status, or family support can be better connected so that families do not have to deal separately with multiple institutions. Success can be measured not only by the number of digital services available, but also by whether families can complete necessary procedures securely and independently, without unnecessary time or caregiving burdens.

Digital-by-default need not mean digital-only. Essential family services can retain assisted channels through face-to-face centers, telephone support, low-data interfaces, accessible design, and multilingual information. Schools, local authorities, civil society organizations, community institutions, and service centers can also help families facing difficulties with digital skills, access, or trust.

Targeted support can complement services available to all. Where affordability, connectivity, or access to appropriate devices creates barriers, relevant policies may provide support for connectivity, devices, accessibility tools, or assisted use. Digital safety initiatives can also be linked with education, skills, and employment programs. Access alone is not sufficient if families lack the knowledge and support needed to use digital services safely, while protection measures may have limited reach if economic and access barriers are overlooked. Meaningful digital inclusion can therefore support not only access to services but also families' participation in education, employment, and wider social and economic life.

6. Create Trusted Reporting, Recovery, and Remedy Mechanisms

Prevention needs to be supported by effective mechanisms for reporting, recovery, and remedy. When digital harm occurs, families need to know where to seek help, what happens after a report is made, how information and evidence will be handled, and where appropriate support is available. Reporting therefore needs to be connected with referral, follow-up, and support rather than ending with the submission of a complaint.

Families and children need clear and accessible routes to assistance. Depending on the nature of the harm, support may include immediate safety advice, preservation of evidence, action by the relevant platform, referral to law enforcement, legal guidance, psychosocial support, school intervention, or social services. These forms of assistance need to be connected through appropriate referral, information-sharing, and follow-up arrangements so that children and families are not left to identify and approach each responsible institution on their own or required to repeatedly recount the same incident when seeking assistance.Reporting and support mechanisms can include child-friendly language, confidentiality or anonymity where appropriate, timely assessment of risks, trained personnel, safe handling of evidence, clear procedures for referral to platforms or law-enforcement authorities, feedback to those seeking help, and follow-up where there is a risk of repeated harm. These elements help connect reporting with the wider protection and support available to children and families (International Telecommunication Union, 2020).
Removing harmful content may be an important part of the response, but it is not always sufficient. Where a child has experienced sexual exploitation, blackmail, cyberbullying, non-consensual image sharing, fraud, or severe harassment, recovery may also require psychosocial, legal, educational, and family support. Effective remedy therefore involves both stopping the harm and supporting the child's recovery and well-being.

Some digital harms also extend across national borders. Where harmful content, fraud, or abuse involves actors, services, or infrastructure in different jurisdictions, cooperation among national authorities, reporting mechanisms, platforms, law-enforcement bodies, and relevant international networks can support timely referral and response. OIC Member Countries can strengthen cooperation in such cases while maintaining clear institutional responsibilities, data-protection safeguards, and referral procedures.

7. Strengthen Anticipatory Governance for Platforms and Emerging Technologies

Digital family governance needs to keep pace with emerging technologies and new forms of digital risk. Regulatory systems focused mainly on established categories of harmful content may not adequately address developments such as generative AI, synthetic media, biometric systems, algorithmic recommendations, conversational agents, immersive environments, and new forms of platform-based commercialization. The aim is not to restrict innovation in advance, but to identify emerging risks early, clarify responsibilities, and adapt safeguards as technologies and patterns of use change.

Existing risk assessment, oversight, and accountability mechanisms need regular review as new technologies and practices emerge. Regulators and other relevant authorities also need sufficient technical expertise to understand significant changes in platform design, recommendation systems, advertising practices, data use, and other developments affecting children and families. Where emerging technologies are used in services

that may significantly affect children and families, particular attention is needed to transparency, human oversight, and access to appeal.

Reporting and protection mechanisms also need to reflect new forms of digitally enabled harm, including synthetic or manipulated intimate content, voice imitation, impersonation, AI-assisted fraud, privacy breaches, and deceptive interactions. Biometric and intimate data require particular attention because their unauthorized disclosure or manipulation may have lasting consequences.

The commercialization of children's digital lives also requires attention. Where parents or third parties commercially share children's lives online, relevant policies need to consider children's privacy and best interests, as well as their economic rights and future ability to seek removal of content. Particular care is needed where financial interests may conflict with the rights and interests of the child.

Regular review involving regulators, researchers, child-development specialists, industry, civil society, parents, and young people can help identify emerging technologies and practices and their possible effects on children and families. The findings can be used to update guidance, reporting mechanisms, and, where necessary, regulatory or policy measures. This allows governance systems to respond to technological change without assuming that every new technology is either inherently harmful or inherently beneficial.

8. Strengthen OIC-Level and International Cooperation on Digital Family Governance

National action is essential, but several digital family governance challenges are difficult to address effectively by individual countries acting alone. Global platforms operate across jurisdictions; harmful content may be hosted abroad; digital services and AI systems may be provided by multinational companies; and countries differ in regulatory, technical, and research capacity. Cooperation among OIC Member Countries, together with wider regional and international cooperation where relevant, can help address these challenges while allowing countries to maintain their own legal and institutional approaches.

Within the OIC, cooperation can include knowledge and experience sharing, capacity-building for regulators and relevant professionals, exchange of multilingual family-safety resources, adaptation and dissemination of high-quality family-oriented digital content and services, technical assistance, cooperation among national hotlines and reporting mechanisms, and comparative analysis of emerging risks and policy responses. Voluntary peer support and technical cooperation can help Member Countries strengthen regulatory, research, and implementation capacities according to national needs and priorities.

Cooperation with major technology companies and other relevant international actors is particularly important for issues that extend across national borders. These include local-language moderation, child-friendly reporting, response times, transparency, evidence preservation, cross-border referral, and access to relevant information for oversight, consistent with applicable legal frameworks. Where appropriate, coordinated engagement among Member Countries may also strengthen their ability to raise common concerns with global platforms.

Cooperation can also support learning across different national systems without requiring countries to replicate particular institutional models. The cases in this report show that similar functions can be performed through different administrative arrangements. Comparative learning can therefore focus on whether the necessary functions—prevention, education, reporting, referral, support, remedy, oversight, and evidence generation—are in place and how they can be adapted to different legal systems, capacities, family structures, and cultural contexts. Beyond the OIC, engagement with relevant regional and international mechanisms can further support responses to cross-border harms, emerging technologies, and other challenges that require cooperation across jurisdictions.

9. Implement Through a Phased Roadmap and Outcome-Based Monitoring

The recommendations need not be introduced as a single reform package. Member Countries can proceed in stages according to their national needs, existing legal and institutional arrangements, available capacities, and policy priorities. The three phases below provide an indicative sequence and timeframe rather than a fixed implementation schedule. Member Countries may adjust both the pace and order of implementation according to their national circumstances.

9.1. Initial Phase (indicatively 0–2 years): Strengthen Foundational Protection and Coordination

National action: Initial efforts can focus on reviewing legal and institutional gaps; strengthening coordination and referral arrangements; establishing or improving accessible and child-friendly reporting and assistance channels; strengthening core platform and data-protection safeguards; providing age-appropriate family digital-literacy support; and establishing baseline evidence on family digital practices and relevant incidents. Monitoring at this stage can focus on the availability and accessibility of essential services, complaint and referral times, awareness of available support, relevant family and child outcomes, and gaps in access.

International Cooperation: Early implementation can be supported through assessment tools, exchange of legal and policy experience, foundational training, peer learning, and technical cooperation. These forms of cooperation can be pursued through OIC/COMCEC mechanisms and, where relevant, other regional and international channels, according to Member Countries' needs and priorities.

9.2. Development Phase (indicatively 3–5 years): Integrate Systems and Expand Family Support

National action: As these foundations are strengthened, countries can improve safety- and privacy-by-design approaches; strengthen coordination in case management and referral; expand parenting, media, AI, and privacy literacy through schools, health and social services, and community-based channels; improve accessible and multichannel public services; strengthen professional and regulatory capacity; and develop more regular evidence on families' digital experiences. Monitoring at this stage can consider parents' confidence in managing digital issues, children's confidence in seeking help, family communication, repeated harm, quality of case resolution, equitable use of services, user trust, and data incidents.

International Cooperation: At this stage, cooperation can place greater emphasis on specialist training, exchange of experience on indicators and evaluation, comparative research, adaptation of relevant resources to different national and linguistic contexts, and cooperation among reporting and support mechanisms.

9.3. Consolidation Phase (indicatively 5+ years): Strengthen Anticipatory and Cross-Border Governance

National action: Over the longer term, countries can strengthen review and evaluation mechanisms; periodically examine the effects of digital policies and services on children and families; improve oversight of AI and algorithmic systems; establish regular processes for identifying emerging technological risks; strengthen arrangements for cross-border reporting and evidence preservation; and maintain the professional and institutional capacity needed to sustain these efforts. Monitoring at this stage can focus on longer-term trends in relevant family and child outcomes, the effectiveness of oversight and cross-border responses, platform accountability, inclusion, and trust.

International Cooperation: Longer-term cooperation can support engagement with major technology companies, cooperation among reporting mechanisms and research networks, continued capacity-building and peer learning, and coordinated responses to emerging technologies and risks that extend across national borders.

Across all three phases, monitoring needs to look beyond the number of activities or services delivered. Figures on training participants, reports received, content removed, or use of digital services remain useful for understanding reach and volume, but they do not by themselves show whether families and children are safer, better supported, or better able to use digital services. Outcome monitoring can therefore consider effective access to support, changes in family and child well-being, confidence in seeking help, parent-child communication, quality and timeliness of complaint resolution, repeated harm, meaningful and independent use of digital public services, user trust, and other outcomes relevant to national priorities. Where appropriate, differences related to age, disability-related access needs, income, geography, and language can also be considered while avoiding unnecessary collection of personal data.

At the national level, the phased priorities can be translated into implementation plans identifying responsible institutions, resources, timeframes, and measurable outcomes. Monitoring and evaluation can be incorporated from the beginning, with relevant contributions from statistical institutions, universities, oversight bodies, civil society, parents, and children, where appropriate.

The overall direction is to move beyond a primary focus on connectivity towards safe, meaningful, inclusive, and value-aligned digital participation for the whole family. Families need to be able to benefit from digital opportunities while responsibility for foreseeable risks is appropriately shared among public authorities, platforms, service providers, institutions, communities, parents, and children according to their respective roles and capacities. Outcome monitoring provides a basis for assessing whether these efforts support family and child well-being and enable families to contribute to wider social and economic development.

These recommendations translate the report's value framework into complementary areas of action aimed at strengthening the family institution in the digital age and supporting its role as a backbone of development. They bring together the protection of family, progeny, and intellect (Hifz), shared responsibility (Mas'uliyyah), prudent and forward-looking governance (Hikmah), and the broader principles of trust, integrity, and balanced digital engagement. Together, these principles provide a common foundation for family-centered digital policies while allowing Member Countries to adapt specific measures to their institutional, legal, social, and cultural contexts.

REFERENCES

Abd Kadir, K., Hoque, M., & Rafindadi, U. B. (2026). Ethics of Qur'anic communication in the era of artificial intelligence: Perspectives from Ibn ʿAshur's Tafsir. Suhuf: International Journal of Islamic Studies, 38(1), 143–153. https://doi.org/10.23917/suhuf.v38i1.16392

Abdallah, F. M., & Hamdan-Mansour, A. M. (2024). Status and sociodemographic correlates of pathological internet use among adolescents in Jordan: A cross-sectional study. *Middle East Current Psychiatry, 31*, Article 69. https://doi.org/10.1186/s43045-024-00459-w

Addati, L., Cattaneo, U., Esquivel, V., & Valarino, I. (2018). *Care work and care jobs for the future of decent work.* International Labour Office. https://www.ilo.org/publications/major-publications/care-work-and-care-jobs-future-decent-work

Adigwe, I. (2021). Identifying the moderating and mediating variables in parental mediation practices in Nigerian families in the digital age. *Social Media + Society, 7*(3), 1–12. https://doi.org/10.1177/20563051211033817

Adigwe, I. (2024). Adolescents' online risks and parental mediation in Nigerian families: Gender in focus. *SAGE Open, 14*(3). https://doi.org/10.1177/21582440241271106

Adigwe, I., & van der Walt, T. (2020). Parental mediation of online media activities of children in Nigeria: A parent-child approach. *Computers in Human Behavior Reports, 2*, 100041. https://doi.org/10.1016/j.chbr.2020.100041

Al-Bukhari, M. I. (2002). *Sahih al-Bukhari*. Dar Ibn Kathir.

Al-Isfahani, R. (n.d.). *Al-Mufradat fi Gharib al-Qur'an* [Dictionary of Qur'anic Terms]. Dar al-Ma'rifah.

Al-Shatnawi, F. E., Ababneh, A. M. T., Elemary, F. M., Rayan, A., & Baqeas, M. H. (2024). Prevalence of cyberbullying perpetration and cyberbullying victimization among nursing students in Jordan. *SAGE Open Nursing, 10*, 23779608241256509. https://doi.org/10.1177/23779608241256509

Al Wahaibi, S., Al-hijji, K., & Raja Hussain, R. M. (2025). Digital citizenship in K-12: International models and lessons for Oman. *IJASOS-International E-Journal of Advances in Social Sciences, 10*(30), 420–429. https://doi.org/10.5281/zenodo.14552287

Al-Zuhayli, W. (2003). *Tafsir al-Munir* (Vol. 3). Dar al-Fikr.

Alarabiat, N. (2024). The influence of the digital age on early childhood in Jordan. *Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 14*, 49–77. https://izlik.org/JA32ET27YL

Ali, F., Bouzoubaa, K., Gelli, F., Hamzi, B., & Khan, S. (2025). Islamic ethics and AI: An evaluation of existing approaches to AI using trusteeship ethics. *Philosophy & Technology, 38*, Article 120. https://doi.org/10.1007/s13347-025-00922-4

Alsaleh, A. (2024). The impact of technological advancement on culture and society. *Scientific Reports, 14*, 32140. https://doi.org/10.1038/s41598-024-83995-z

Alshakhsi, S., Al-Harahsheh, S., Hassan, D. A., Al-Thani, D., & Ali, R. (2025). Digital addiction among Arab families: Status, contributing factors, responsibilities, and solutions. *Communications of the ACM*. https://cacm.acm.org/arab-world-regional-special-section/digital-addiction-among-arab-families-status-contributing-factors-responsibilities-and-solutions/

Altalib, H., AbuSulayman, A. H., & Altalib, O. (2024). *Parent-child relations: A guide to raising children* (Rev. ed.). The International Institute of Islamic Thought (IIIT).

Alwi, N. H. M., Norwawi, N. M., Ismail, R., Wahid, F., & Alkaenay, N. M. (2014). Promoting Islamic ethics on privacy in digital social network for user data protection and trust. Ulum Islamiyyah, 13, 115–127.

Ammari, L. H. (2025, November 22). Digital guardianship: Using AI to protect Jordan's heritage. *The Jordan Times*. https://jordantimes.com/opinion/lubna-hanna-ammari/digital-guardianship-using-ai-to-protect-jordans-heritage

Amnesty International. (2024). *Jordan: New Cybercrimes Law stifles freedom of expression and assembly*. https://www.amnesty.org/en/documents/mde16/8424/2024/en/

ASEAN ICT Forum. (2024). *Achievements 2012–2024 of Click Wisely programme and digital safety awareness initiatives in Malaysia*. https://aseanictforum.com/

ASEAN ICT Forum. (2024). *Regional perspectives on digital literacy and child online protection across Southeast Asia*. ASEAN Secretariat.

Auda, J. (2008a). *Maqāṣid al-Sharīʿah as philosophy of Islamic law: A systems approach*. The International Institute of Islamic Thought (IIIT).

Auda, J. (2008b). *Maqasid al-Shariah: A beginner's guide*. The International Institute of Islamic Thought (IIIT).

Auladi, G. A., & Muwahid, F. (2025). Cybersecurity and moral responsibility: A philosophical-Islamic approach to digital trust. *TechComp Innovations: Journal of Computer Science and Technology*, 2(1), 53–65. https://doi.org/10.70063/techcompinnovations.v2i1.93

Austin, L. (2020, December 22). *Who decides? Consent, meaningful choices, and accountability*. https://srinstitute.utoronto.ca/news/austin-consent-meaningful-choice-accountability

Bakar, O. (2014). *Islamic civilisation and the modern world: Thematic essays*. UTM Press.

Bărbuță, A., Ghețău, C., & Iovu, M.-B. (2023). Digital technology and family dynamics: The 3Rs conceptual model regarding the acceptance and use of digital technology in everyday family routines. *East European Journal of Society and Politics*, 9(1), 120–144. https://doi.org/10.17356/ieejsp.v9i1.1049

Bayzan, Ş. (n.d.). *Dünyada ve Türkiye'de güvenli internet merkezleri*. https://www.guvenliweb.org.tr/blog-detay/dunyada-ve-turkiyede-guvenli-internet-merkezleri

Bektaş, Ç. (2018). *İşletme organizasyonu*. Beta.

Benedetto, L., & Ingrassia, M. (2021). Digital parenting: Raising and protecting children in media world. In *Parenting - Studies by an Ecocultural and Transactional Perspective*. IntechOpen. https://doi.org/10.5772/intechopen.92579

Better Internet for Kids. (2024). *Digital child protection strategy of Hungary (DGYS)*. European Commission. https://better-internet-for-kids.europa.eu/en/knowledge-hub/rules-guidelines/digital-child-protection-strategy-hungary-dgys

Better Internet for Kids. (2025a). *Act LXXVIII of 2024 on the suppression of Internet Aggression*. European Commission. https://better-internet-for-kids.europa.eu/en/rules-guidelines/act-lxxviii-2024-suppression-internet-aggression

Better Internet for Kids. (2025b). *BIK policy monitor country profile 2025: Hungary*. European Commission. https://better-internet-for-kids.europa.eu/sites/default/files/2025-07/HU%20Country%20Profile%202025_final-upd17072025.pdf

Better Internet for Kids. (2026). *Hungarian Safer Internet Centre*. European Commission. https://better-internet-for-kids.europa.eu/en/sic/hungary

Better Internet for Kids. (2026). *SIC+ programme: Egypt - National Council for Childhood and Motherhood*. https://better-internet-for-kids.europa.eu/en/sic/egypt

Bietti, E. (2021). A genealogy of digital platform regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3859487

Bilgi Teknolojileri ve İletişim Kurumu. (2019, June 11). *Güvenli internet hizmeti*. https://internet.btk.gov.tr/guvenli-internet-hizmeti

Bradford, N. K., Caffery, L. J., & Smith, A. C. (2016). Telehealth services in rural and remote Australia: A systematic review of models of care and factors influencing success and sustainability. *Rural and Remote Health, 16*, 3808. https://doi.org/10.22605/RRH3808

Brandtzaeg, P. B., Skjuve, M., & Følstad, A. (2022). My AI friend: How users of a social chatbot understand their human–AI friendship. *Human Communication Research, 48*(3), 404–429. https://doi.org/10.1093/hcr/hqac008

Bronfenbrenner, U. (1979). *The ecology of human development: Experiments by nature and design*. Harvard University Press.

Carvalho, J., Francisco, R., & Relvas, A. P. (2015). Family functioning and information and communication technologies: How do they relate? A literature review. *Computers in Human Behavior, 45*, 99–108. https://doi.org/10.1016/j.chb.2014.11.037

Chang, F. C., Miao, N. F., Chiu, C. H., Chen, P. H., Lee, C. M., Chiang, J. T., & Chuang, H. Y. (2016). Urban–rural differences in parental Internet mediation and adolescents' Internet risks in Taiwan. *Health, Risk & Society, 18*(3–4), 188–204. https://doi.org/10.1080/13698575.2016.1190002

Coleman, J. S. (1988). Social capital in the creation of human capital. *American Journal of Sociology, 94*, S95–S120. https://doi.org/10.1086/228943

Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25)*. United Nations. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

Communications and Multimedia Act 1998 (Act 588). (1998). Government of Malaysia.

Conger, R. D., Conger, K. J., & Martin, M. J. (2010). Socioeconomic status, family processes, and individual development. *Journal of Marriage and Family, 72*, 685–704. https://doi.org/10.1111/j.1741-3737.2010.00725.x

Content Forum. (n.d.). *Content Forum Malaysia*. https://contentforum.my/

Convention on children's rights in the digital world. (2026). https://enstitusosyal.org/imza

Council of Europe. (2026). *Jordan: Octopus Cybercrime Community country profile*. https://www.coe.int/en/web/octopus/-/jordan

Cullen, R. (2001). Addressing the digital divide. *Online Information Review, 25*(5), 311–320.

CyberSAFE Malaysia. (2023). *License2Surf and CyberSAFE Parents platforms*. https://www.cybersafe.my

CyberSecurity Malaysia. (2023a). *CyberSAFE programme overview and cyber security awareness initiatives*. https://www.cybersecurity.my

CyberSecurity Malaysia. (2023b). *National cyber security awareness and CyberSAFE framework annual report*. CyberSecurity Malaysia.

CyberSecurity Malaysia. (2024). *MyCERT (Malaysian Computer Emergency Response Team): Cyber incident response and Cyber999 services overview*. https://www.mycert.org.my

DataReportal. (2025, March 3). *Digital 2025: Nigeria*. https://datareportal.com/reports/digital-2025-nigeria

DataReportal. (2025, November 8). *Digital 2026: Hungary*. https://datareportal.com/reports/digital-2026-hungary

DataReportal. (2025, November 8). *Digital 2026: Jordan*. https://datareportal.com/reports/digital-2026-jordan

De Veirman, M., Cauberghe, V., & Hudders, L. (2017). Marketing through Instagram influencers: The impact of number of followers and product divergence on brand attitude. *International Journal of Advertising, 36*(5), 798–828. https://doi.org/10.1080/02650487.2017.1348035

Deak, Z., Karlovitz, T. J., & KárpátiDaróczi, J. (2024). Digital communication patterns in families: Generational and country of origin effects. *Acta Polytechnica Hungarica, 21*(8), 309–329. https://doi.org/10.12700/APH.21.8.2024.8.16

Department of Statistics. (2025). *Estimated population of the Kingdom by administrative divisions, at the end of 2025*. https://dosweb.dos.gov.jo/DataBank/population/population_Estimares/PopulationEstimates.pdf

Department of Statistics. (2025). *Jordan statistical yearbook 2025*. Government of Jordan. https://dosweb.dos.gov.jo/product/jordan-statistical-yearbook-2025/

Department of Statistics Malaysia. (2026). *Current population estimates, Malaysia, 2026*. https://www.dosm.gov.my

Department of Statistics, Ministry of Health, & ICF. (2024). *Jordan Population and Family Health Survey 2023*. Department of Statistics and ICF. https://dosweb.dos.gov.jo/?p=35453&post_type=product

Digital Citizenship Programme. (2026). *Digital citizenship: Programme and mobile application services*. Government of Hungary. https://app.dap.gov.hu/en/program

Digital for Life. (2026). *Our programmes and projects*. https://www.digitalforlife.gov.sg/about/our-projects

Digwatch. (2022, August). *Hungary's national digitalisation strategy 2022–2030*. https://dig.watch/resource/hungarys-national-digitalisation-strategy-2022-2030

Diyanet Radio. (2026). *Children's tales* [Radio program]. https://diyanetradyo.com/programlar/cocukca-masallar

Dukeh, S. (2026, January 10). What is Nigerian family life like? *The Guardian*. https://guardian.ng/nigerian/what-is-nigerian-family-life-like/

Economic Planning Unit. (2021). *Malaysia digital economy blueprint*. Prime Minister's Department, Malaysia.

ECPAT International. (2022). *Sexual exploitation of children in Nigeria: Country overview*. https://ecpat.org/country/nigeria/

ECPAT International, & UNICEF. (2022). *Disrupting harm in Malaysia: Evidence on online child sexual exploitation and abuse*. ECPAT International & UNICEF East Asia and Pacific Regional Office.

Egielewa, P. E., & Umolu, P. E. (2022). Digital-mediated communication: Effect of smartphone use on family communication in Nigeria. *International Journal of Arts and Technology, 14*(3), 206–223. https://doi.org/10.1504/IJART.2022.128462

Eira, M., Rasouli, A., & Charisi, V. (2025). Parents' perceptions about the use of generative AI systems by adolescents. In *Proceedings of the 24th Interaction Design and Children* (pp. 927–931).

European Commission. (2025, June 17). *State of the digital decade 2025: Keep building the EU's sovereignty and digital future*. https://data.consilium.europa.eu/doc/document/ST-10407-2025-INIT/en/pdf

European Commission. (2025, June 18). *Hungary 2025 digital decade country report*. https://digital-strategy.ec.europa.eu/en/factpages/hungary-2025-digital-decade-country-report

European Commission. (2025, May 22). *User rights under the Digital Services Act*. https://digital-strategy.ec.europa.eu/en/factpages/user-rights-under-digital-services-act

European Commission. (2026). *Hungary's 2026 Digital Decade country report*. https://digital-strategy.ec.europa.eu/en/factpages/hungarys-2026-digital-decade-country-report

European Commission. (2026, March 31). *Digital connectivity in Hungary*. https://digital-strategy.ec.europa.eu/en/policies/digital-connectivity-hungary

European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. (2022). *Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act)*. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

European Union. (2026). *General Data Protection Regulation*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504#tit_1

Fam, J. Y., Juhari, R., Kääriäinen, M., & Männikkö, N. (2025). Reconsidering parental mediation with new media technology. *Frontiers in Human Dynamics, 7*, 1495954. https://doi.org/10.3389/fhumd.2025.1495954

Family- and child-friendly productions and series promotion regulation. (2018, May 8). *Official Gazette* (No. 30415). https://www.resmigazete.gov.tr/eskiler/2018/05/20180508-4.html

Fardouly, J., & Vartanian, L. R. (2016). Social media and body image concerns: Current research and future directions. *Current Opinion in Psychology, 9*, 1–5. https://doi.org/10.1016/j.copsyc.2015.09.005

Federal Ministry of Communications and Digital Economy. (2020). *National Digital Economy Policy and Strategy (2020–2030)*. Federal Republic of Nigeria.

Federal Republic of Nigeria. (2003). *Child Rights Act, 2003*.

Federal Republic of Nigeria. (2015). *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015*.

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*. https://ndpc.gov.ng/wp-content/uploads/2024/03/Nigeria_Data_Protection_Act_2023.pdf

Federal Republic of Nigeria. (2024). *Cybercrimes (prohibition, prevention, etc.) (Amendment) Act, 2024*.

Federal Trade Commission. (2002). *Protecting children's privacy under COPPA: A survey on compliance*. https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences, 9*(2), 127–152.

Fischhoff, B., Watson, S. R., & Hope, C. (1984). Defining risk. *Policy Sciences, 17*(2), 123–139.

Genç, N. (2012). *Yönetim ve organizasyon – Çağdaş sistemler ve yaklaşımlar*. Seçkin Yayıncılık.

Goode, W. J. (1963). *World revolution and family patterns*. Free Press of Glencoe.

GOV UK. (2025). *Online Safety Act: Explainer*. https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

Government of Hungary. (2011/2026). *The Fundamental Law of Hungary* (consolidated English translation). National Legislation Database. https://njt.hu/jogszabaly/en/2011-4301-02-00

Government of Hungary. (2016). *Digital Child Protection Strategy of Hungary*. Government Decree 1488/2016 (IX. 2). https://digitalisjoletprogram.hu/files/c2/61/c2610c5560ef56425860d4d7bdd68b3d.pdf

Government of Hungary. (2023). *Act CIII of 2023 on the digital State and certain rules for the provision of digital services*. National Legislation Database. https://njt.hu/translations

Government of Jordan. (2022). *Economic Modernisation Vision: Unleashing potential to build the future*. https://jordanvision.jo/en

Grusec, J. E. (2011). Socialization processes in the family: Social and emotional development. Annual Review of Psychology, 62, 243–269. https://doi.org/10.1146/annurev.psych.121208.131650

Güvenli İnternet Merkezi. (2026). *Hakkımızda*. https://www.gim.org.tr/hakkimizda.php

Had, A., & Ationg, R. (2026). The impact of digital transformation on society in Malaysia: A literature-based study of social behaviour and identity. Asian Journal of Research in Education and Social Sciences, 8(1), 643–658.

Hadasik, B., & Mach-Król, M. (2024). On enhancing the COVID-19 certification system for the digitally-illiterate people inclusion in the European Union. *Digital, 4*(1), 182–194. https://doi.org/10.3390/digital4010009

Halász, C. (2025). Children in digital age – Hungarian perspective. In C. Halász (Ed.), *Children in digital age* (pp. 153–169). Central European Academic Publishing. https://doi.org/10.71009/2025.csh.cida_8

Han, B. C. (2015). *The transparency society*. Stanford University Press.

Hashemite Kingdom of Jordan. (1952/2022). *The Constitution of the Hashemite Kingdom of Jordan*. https://istd.gov.jo/EBV4.0/Root_Storage/EN/EB_Pages/Constitution_of_the_Hashemite_Kingdom_of_Jordan.pdf

Hashemite Kingdom of Jordan. (2023). *Cybercrime Law No. 17 of 2023. Official Gazette*. https://pm.gov.jo/Ar/Pages/NewsPaperDetails/5874

Holland, G., & Tiggemann, M. (2016). A systematic review of the impact of the use of social networking sites on body image and disordered eating outcomes. *Body Image, 17*, 100–110. https://doi.org/10.1016/j.bodyim.2016.02.008

Hungarian Central Statistical Office. (2025). *Statistical pocketbook of Hungary, 2024*. https://www.ksh.hu/evkonyvek/2024/magyar-statisztikai-zsebkonyv-2024/pdf/statistical_pocketbook_of_hungary_2024.pdf

Hungarian Central Statistical Office. (2026). *Population and vital events*. https://www.ksh.hu/population-and-vital-events

Hungarian Central Statistical Office. (2026). *Statistical pocketbook of Hungary, 2025*. https://www.ksh.hu/evkonyvek/2025/magyar-statisztikai-zsebkonyv-2025/pdf/statistical_pocketbook_of_hungary_2025.pdf

Hungary Today. (2023). *Campaign launched for children's online safety*. https://hungarytoday.hu/campaign-launched-for-childrens-online-safety/

Hussin, S. B. H. (2025). Islamic digital civilisation: Challenges and opportunities in shaping the values and ethics of the Ummah. *International Journal of Islam and Contemporary Affairs*, 5(2), 123–142. https://doi.org/10.61465/jurnalyadim.v5.345

Ibrahim, N. N., & Halim, H. (2025). Do smartphones replace family communication? *Proceedings of the 9th International Conference on Communication and Media (i-COME 24)*, 67–74. Atlantis Press. https://doi.org/10.2991/978-94-6463-756-4_7

IMF Data. (n.d.). *World economic outlook database*. https://data.imf.org/en/Data-Explorer?datasetUrn=IMF.RES:WEO(9.0.0)

İnan, M., & Demir, M. (2018). Eğitimde fırsat eşitliği ve kamu politikaları: Türkiye üzerine bir değerlendirme. *Ankara Hacı Bayram Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 20*(2), 337–359. https://izlik.org/JA43ST69UW

Information and Communication Technologies Authority. (2026). *Market data report on the electronic communications sector in Türkiye*. https://www.btk.gov.tr/s3/web-btk-site/7708c26c-5161-4919-8b3d-daa31d4ac8fb/2026/06/46150l5e-244a-4bb4-bfd3-937cf9480229.pdf

Information and Communication Technologies Authority. (2026). *Safe Play*. https://www.guvenlioyna.org.tr/

Information and Communication Technologies Authority. (2026). *Safer Internet Center*. https://www.gim.org.tr

INHOPE. (2025). *Annual report 2024*. https://www.inhope.org/media/pages/home/data-insights/4d2f6f4817-1767872796/inhope-annual-report-2024.pdf

Innocenti UNICEF. (2025). *Guidance on AI and Children 3.0: Updated guidance for governments and businesses to create AI policies and systems that uphold children's rights*. UNICEF Innocenti–Global Office of Research and Foresight.

International Telecomination Union. (2026). *Nigeria*. https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Pages/projects/Job-Skills/countries/Nigeria.aspx

International Telecommunication Union. (2020). *Guidelines for policy-makers on child online protection*. https://www.itu.int/pub/S-GEN-COP.POL_MAKERS-2020

International Telecommunication Union. (2022). *Global cybersecurity index 2022*. ITU.

International Telecommunication Union. (2023). *Measuring digital development: Facts and figures 2023*. https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/

Internet Hotline. (2026). *About us*. https://ihbarweb.org.tr/eng/about.html

Iqbal, M., & Kanus, O. (2026). Qur'anic foundations of digital adab: A thematic exegesis and its implications for Islamic religious education in the digital age. AL-ADABIYAH: Jurnal Pendidikan Agama Islam, 7(4)

International Telecommunication Union. (2020). Guidelines for parents and educators on child online protection. ITU.

International Telecommunication Union. (2022). Guidelines for utilization of the Global Cybersecurity Agenda by the ITU. ITU.

International Telecommunication Union. (2023). Kazakhstan's Digital Family Card: Ensuring equal access to social protection. ITU.

Iyanda, V. F., & Adegbite, A. E. (2025). Child protection in Nigeria's digital era: Socio-legal perspectives on online exploitation, and the role of social work. *Lead City University Law Journal (LCULJ)*, *7*(1), 234–250. https://doi.org/10.5281/zenodo.17974591

Javor, B. (2025, December 1). *EU report on Hungary's digital transformation: The pace is good, but let's speed up!* https://www.oeconomus.hu/en/oecofocus/eu-report-on-hungarys-digital-transformation-the-pace-is-good-but-lets-speed-up/

Jordan News Agency (Petra). (2026, April 26). *Minister launches 'Fortify' initiative to enhance child digital protection*. https://org.petra.gov.jo/Include/InnerPage.jsp?ID=83888&lang=en&name=en_news

Jordan Open Source Association. (2023). *Full text in English of the Cybercrime Law of 2023 (unofficial translation)*. https://www.josa.ngo/publications/33

Jordan River Foundation. (2024). *JRF's 110 helpline*. https://www.jordanriver.jo/en/programs/protecting-children/110-families-children

Jordan River Foundation. (n.d.-a). *Public awareness campaigns*. https://www.jordanriver.jo/en/programs/jrf%E2%80%99s-child-safety-program/public-awareness-campaigns

Jordan River Foundation. (n.d.-b). *110 Families and children helpline*. https://www.jordanriver.jo/en/programs/protecting-children/110-families-children

Jordan River Foundation. (n.d.-c). *JRF's child safety program*. https://www.jordanriver.jo/en/programs/jrf%E2%80%99s-child-safety-program

Jordan River Foundation. (n.d.-d). *Strengthening JRF's 110 helpline & online case management services*. https://www.jordanriver.jo/en/programs/jrf%E2%80%99s-child-safety-program/strengthening-jrf%E2%80%99s-110-helpline-online-case-management-services

Jordan River Foundation & UNICEF Jordan. (2021, December 14). *JRF, UNICEF call for laws to protect children from online exploitation*. https://www.jordanriver.jo/en/media/news/jrf-unicef-call-laws-protect-children-online-exploitation

Jordan Times. (2026a, June 16). SANAD app users rising—Ministry. *The Jordan Times*. https://jordantimes.com/news/business/sanad-app-users-rising-ministry

Kadir, M. R. A. (2025). Islamic technology: A paradigm shift in science & technology. *Journal of Islamic Technology, 1*(1). https://unissa.edu.bn/journal/index.php/JIT/article/view/1148

Kadir, M. R. A. (2025). Islamic technology: A paradigm shift in science & technology. *Journal of Islamic Technology, 1*(1). Retrieved from https://unissa.edu.bn/journal/index.php/JIT/article/view/1148

Kalın, İ. (2010). Medeniyet kavramı ve İslam medeniyeti. *Divan: Disiplinlerarası Çalışmalar Dergisi, 15*(29), 1–24.

Kamali, M. H. (2015). *The middle path of moderation in Islam: The Qur'anic principle of Wasatiyyah*. Oxford University Press.

Kamali, M. H. (2019). *The objectives of Shariah (Maqasid al-Shariah): A textbook*. Islamic Book Trust.

Karjalainen, T. (2022). The battle of power: Enforcing data protection law against companies holding data power. *Computer Law & Security Review, 47*, 105742. https://doi.org/10.1016/j.clsr.2022.105742

Kasim, A. C., Dien, M. I., Kasim, S. C., & Manap, J. (2020). The impact of amanah on individual manners and the society. *International Journal of Academic Research in Business and Social Sciences, 10*(9), 629–640. https://doi.org/10.6007/IJARBSS/v10-i9/7854

Kasim, A., et al. (2020). Digital ethics and shared governance: Institutional obligations in the digital age. *Journal of Media and Ethics, 35*(2), 110–124.

Kasim, N. A. A., Yusof, M. F. M., Ahmad, M. H., & Ibrahim, M. (2020). The impact of amanah on individual manners and the society. *International Journal of Academic Research in Business and Social Sciences, 10*(9), 631–640.

Kenyeres, K. (2025). *Hungarian family values and policies discussed by experts and policymakers*. https://www.elfac.org/family-values-and-policies-discussed-by-experts-and-policymakers-at-family-2025-conference

KINCS. (2025a, January 31). *Family 2025*. Mária Kopp Institute for Demography and Families. https://www.koppmariaintezet.hu/en/allarticles/835-family-2025

KINCS. (2025b). *Our institute*. Mária Kopp Institute for Demography and Families. https://www.koppmariaintezet.hu/en/intro

KINCS (Mária Kopp Institute). (2021). *Project Europe - family issues: Hungary is one of the most family centered nations*. https://www.koppmariaintezet.hu/en/allarticles/474-project-europe-family-issues-hungary-is-one-of-the-most-family-centered-nations

KINCS (Mária Kopp Institute). (2025). *European Union family policy outlook & societal value barometer*. KINCS International Publications.

Koçel, T. (2020). *İşletme yöneticiliği*. Beta.

Komanchuk, J., Toews, A. J., Marshall, S., Mackay, L. J., Hayden, K. A., Cameron, J. L., Duffett-Leger, L., & Letourneau, N. (2023). Impacts of parental technoference on parent–child relationships and child health and developmental outcomes: A scoping review. Cyberpsychology, Behavior, and Social Networking, 26(8), 579–603.

Konrad, C., Berger-Hanke, M., Hassel, G., & Barr, R. (2021). Does texting interrupt imitation learning in 19-month-old infants? Infant Behavior and Development, 62, 101513.

Konok, V., Bunford, N., & Miklósi, Á. (2020). Associations between child mobile use and digital parenting style in Hungarian families. *Journal of Children and Media, 14*(1), 91–109. https://doi.org/10.1080/17482798.2019.1684332

Kutluer, İ. (1998). Hikmet. In *TDV İslâm Ansiklopedisi* (Vol. 17, pp. 503–511). Türkiye Diyanet Vakfı İslâm Araştırmaları Merkezi.

Law No. 6112 on the establishment and broadcasting services of radio and television organizations. (2011, March 3). https://mevzuat.gov.tr/mevzuat?MevzuatNo=6112&MevzuatTur=1&MevzuatTertip=5

Law No. 7578 on social services and amendments to certain laws. (2026, May 1). *Official Gazette* (No. 33240). https://www.resmigazete.gov.tr/eskiler/2026/05/20260501-1.html

Laws of Malaysia. (2025). *Online Safety Act 2025 (Act 866)*, Part II, Section 5. Commissioner of Law Revision, Malaysia.

Malaysian Communications and Multimedia Commission. (2023). *Klik Dengan Bijak (Click Wisely) programme overview and digital awareness initiatives*. https://www.mcmc.gov.my

Lee, S. Y. (2023, September 23). *Discourses of digital citizenship in K-12 education in South Korea*. Presented at the 1st International Conference on The Citizenship Education of The Digital Era, Srinakharinwirot University, Thailand.

Liu, J., & Tan, E. (2025). *Positive use guide: Evidence-based insights on the impact of digital devices on child and adolescent wellbeing*. Centre for Evidence and Implementation.

Livingstone, S., & Blum-Ross, A. (2020). *Parenting for a digital future: How hopes and fears about technology shape children's lives*. Oxford University Press.

Livingstone, S., & Blum-Ross, A. (2020). *Parenting for a Digital Future: How the Hopes and Fears of Parents Shape Children's Technology Lives*. Oxford University Press.

Madianou, M., & Miller, D. (2012). *Migration and new media: Transnational families and polymedia*. Routledge.

Malak, M. Z., Khalifeh, A. H., & Shuhaiber, A. H. (2017). Prevalence of Internet addiction and associated risk factors in Jordanian school students. *Computers in Human Behavior, 70*, 556–563. https://doi.org/10.1016/j.chb.2017.01.011

McDaniel, B. T., & Radesky, J. S. (2018). Technoference: Parent distraction with technology and associations with child behavior problems. *Child Development, 89*(1), 100–109. https://doi.org/10.1111/cdev.12822

Ministry of Digital Economy and Entrepreneurship. (2023a). *Personal Data Protection Law No. 24 of 2023*. Government of Jordan. https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/pdpl.pdf

Ministry of Digital Economy and Entrepreneurship. (2023b). *Jordan's Artificial Intelligence Strategy and Implementation Plan 2023–2027*. Government of Jordan. https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/40435648.pdf

Ministry of Digital Economy and Entrepreneurship. (2025a). *Jordanian Digital Inclusion Policy 2025*. Government of Jordan. https://www.modee.gov.jo/En/List/Legislation_and_policies

Ministry of Digital Economy and Entrepreneurship. (2025b). *Data Protection Impact Assessment (DPIA) Guideline*. Government of Jordan. https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/data_protection_impact_assessment_%28dpia%29_guideline.pdf

Ministry of Digital Economy and Entrepreneurship. (2025c). *Data Protection Officer accreditation criteria and registration instructions*. Government of Jordan. https://www.modee.gov.jo/En/List/Legislation_and_policies

Ministry of Digital Economy and Entrepreneurship. (2026a). *Results of the 2024 Household ICT Usage and Access Survey*. Government of Jordan. https://jordan.gov.jo/EN/NewsDetails/Ministry_of_Digital_Economy_and_Entrepreneurship_Announces_Results_of_the_2024_Household_ICT_Usage_and_Access_Survey

Ministry of Digital Economy and Entrepreneurship. (2026b). *Jordanian Digital Transformation Strategy and Implementation Plan 2026–2028*. Government of Jordan. https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/jordanian_digital_transformation_strategy_and_the_implementation_plan_2026-2028.pdf

Ministry of Digital Economy and Entrepreneurship. (2026c). *Directorate of Strategies, Future, and Entrepreneurship: Inclusion Unit*. https://modee.gov.jo/En/Pages/Policies_and_Strategies_Directorate

Ministry of Digital Economy and Entrepreneurship. (n.d.). *Youth, Technology and Jobs project*. https://www.modee.gov.jo/EN/Pages/Youth_Technology_and_Jobs_Project

Ministry of Family and Social Services. (2021). *Türkiye family structure survey*.

Ministry of Family and Social Services. (2023). *Türkiye child rights strategy document and action plan (2023–2028)*. https://ulusaleylem.aile.gov.tr/media/55wftiap/tu-rkiye-c-ocuk-hakları-strateji-belgesi-ve-eylem-planı.pdf

Ministry of Family and Social Services. (2024). *Gambling addiction and family guide*. https://www.aile.gov.tr/media/281221/kumar-bagimliligi-ve-aile-rehberi-17-2.pdf

Ministry of Family and Social Services. (2024). *Vision document and action plan for the protection and strengthening of the family (2024–2028)*. https://aile.gov.tr/media/165130/ailenin-korunmasi-ve-gu-c-lendirilmesi-vizyon-belgesi-ve-eylem-plani.pdf

Ministry of Family and Social Services. (2026). *Action plan for the empowerment of children in the digital world (2026–2030)*. https://www.aile.tr/media/295195/dijital-dunyada-cocuklarin-guclendirilmesine-yonelik-eylem-plani.pdf

Ministry of Family and Social Services. (2026). Action plan for the empowerment of children in the digital world (2026–2030). https://www.aile.tr/media/295195/dijital-dunyada-cocuklarin-guclendirilmesine-yonelik-eylem-plani.pdf

Ministry of Family and Social Services. (2026). *Awareness training program for strengthening and developing children's life skills*. https://akademi.aile.gov.tr/EducationDetail/94/

Ministry of Family and Social Services. (2026). *Children are safe*. https://cocuklarguvende.gov.tr

Ministry of Family and Social Services. (2026). *Family Education Program*. https://aep.aile.gov.tr

Ministry of Family and Social Services. (2026). *Guide to protection from cybercrime and cyberbullying*. https://aile.gov.tr/media/210321/siber-suc-tan-ve-zorbaliktan-korunma-rehberi_flipbook_du-zenleme-1.pdf

Ministry of Family and Social Services. (2026). *My first teacher is my family* [Mobile application]. Google Play.

Ministry of Family and Social Services. (2026). *My safe Internet*. https://www.aile.gov.tr/media/194157/benim-gu-venli-internetim.pdf

Ministry of Family and Social Services. (2026). *Parental guide for protecting children from digital risks*. https://www.aile.tr/media/210313/di-ji-tal_ebeveyn-rehberi_flipbook-1.pdf

Ministry of Interior of the United Arab Emirates. (2024, April 25). *Headed by Saif bin Zayed, Council for Digital Quality of Life adopts 38 indicators*. https://moi.gov.ae/en/media.center/news/042524n01.aspx

Ministry of Interior of the United Arab Emirates. (2025, July 21). *Artificial intelligence for safer children*. https://moi.gov.ae/en/about.moi/Initiative/072125m01.aspx

Ministry of National Education. (2018a). *Medya okuryazarlığı dersi öğretim programı*. https://mufredat.meb.gov.tr/

Ministry of National Education. (2018b). *Bilişim teknolojileri ve yazılım dersi öğretim programı*. https://mufredat.meb.gov.tr/

Ministry of Planning and International Cooperation. (2022). *Public administration modernization roadmap*. https://www.mop.gov.jo/EN/Pages/Public_Sector_Modernization_The_Roadmap?View=4145

Ministry of Trade. (2026). *Nijerya pazara giriş rehberi*. https://ticaret.gov.tr/data/62c696dd13b876ae383fd792/Nijerya%20Pazara%20Giri%C5%9F%20Rehberi.pdf

Muhammad, M. R. (2026). Digital adab: Transposing classical adab to the digital age. KICT Newsletter: SPECTRUM, (5), 7–12.

Mohamed, S. (2025). *Platform Keibubapaan Digital (Platform KID): Content template and guideline*. Communication and Media Centre (COMET), AbdulHamid AbuSulayman Kulliyyah of Islamic Revealed Knowledge and Human Sciences, International Islamic University Malaysia.

Mohamed, S., Janon, N. S., Yusoh, M. H., Salleh, N., Mohd Nasir, N. S., & Wan Mohd Ghazali, W. N. (2025). Designing and evaluating a culturally grounded digital parenting initiative in Malaysia. *Intellectual Discourse, 33*(3), 993–1015. https://doi.org/10.31436/id.v33i3.2433

Mohamed, S., Wok, S., Wan Mohd Ghazali, W. N., & Mohd Nasir, N. S. (2022). Factors influencing the digital parenting styles of Malaysian parents. *International Journal for Studies on Children, Women, Elderly and Disabled, 17*, 24–31.

Mukhamedkaziy, N., Maratova, A., & Mustafin, A. (2025). Digitalization in Kazakhstan. In I. Qoraboyev & Z. Bekshora (Eds.), *CEGREG Yearbook: Central Asia in global and regional governance* (pp. 105–119). Maqsut Narikbayev University.

MyCERT. (2024). *Annual incident management and Cyber999 operational report*. CyberSecurity Malaysia.

Naudeau, S., Kataoka, N., Valerio, A., Neuman, M. J., & Elder, L. K. (2011). Investing in young children: An early childhood development guide for policy dialogue and project preparation. World Bank.

Nashwan, A. J. (2025). Data endowment as a digital waqf: An Islamic ethical framework for AI development. *Philosophy & Technology, 38*, Article 74. https://doi.org/10.1007/s13347-025-00905-5

National Assembly of Nigeria. (2025a). *A bill for an Act to provide for the enactment of Child Online Access Protection and other issues of online violence against the Nigerian child and for related matters (HB. 244)*.

National Assembly of Nigeria. (2025b, November 18). *House of Representatives order paper: Consideration of report on HB. 244*. https://nass.gov.ng/documents/download/11223

National Council for Family Affairs. (2018). *Jordanian family in Jordan 2018*. https://haqqi.info/sites/default/files/2019-04/NCFA_FamilyReport_2018.pdf

National Council for Family Affairs. (2020). *Policies and guiding principles for the prevention of and response to violence in Jordan*. https://ncfa.org.jo/

National Council for Family Affairs. (2022). *Child Rights Law No. 17 of 2022*. https://coj.ncfa.org.jo/EN/Pages/Child_Rights_Law_2022

National Council for Family Affairs. (2023). *Annual report 2023*. https://ncfa.org.jo/

National Council for Family Affairs. (2024). *Annual report 2024*. https://ncfa.org.jo/

National Council for Family Affairs. (2026). *The National Multi-Sectoral Action Plan 2026–2030*. https://ncfa.org.jo/EN/List/Policies_And_Legislation

National Council for Family Affairs. (n.d.-a). *Children of Jordan website*. https://ncfa.org.jo/EN/Pages/Children_of_Jordan_Website

National Council for Family Affairs. (n.d.-b). *Early childhood portal*. https://ncfa.org.jo/EN/Pages/Early_Childhood_Portal

National Council for Family Affairs. (n.d.-c). *Osraty app*. https://www.ncfa.org.jo/

National Council for Family Affairs & UNICEF Jordan. (2021). *National study on violence against children in Jordan*. https://www.unicef.org/jordan/media/9181/file/UNICEF%20VAC%20Report-ENG.pdf

National ICT Security Discourse and Exhibition (NICTSeD). (2025). *CyberSAFE and national cyber awareness activities*. https://www.cybersafe.my/nictsed/about.html

National ICT Security Discourse and Exhibition (NICTSeD). (2025). *National ICT security education and digital capital development strategy (2021–2025)*. Ministry of Communications and Digital.

National Information Technology Development Agency. (2023). *National Digital Literacy Framework*. NITDA.

National Information Technology Development Agency. (2024). *Strategic Roadmap and Action Plan 2024–2027 (SRAP 2.0)*. https://nitda.gov.ng/wp-content/uploads/2024/02/SRAP-2.O.pdf

National Information Technology Development Agency. (n.d.). *3 Million Technical Talent (3MTT)*. https://3mtt.nitda.gov.ng/

National Information Technology Development Agency. (n.d.). *Digital Literacy for All (DL4ALL)*. https://dl4all.nitda.gov.ng/

National Media and Infocommunications Authority. (2021, November 10). *NMHH research: Hungarian children start to use internet younger and younger, but third of parents see no need to enhance digital literacy*. https://english.nmhh.hu/article/224644/

National Media and Infocommunications Authority. (2023). *Building the Net-Coach community*. https://english.nmhh.hu/article/246171/Building_the_NetCoach_community

National Media and Infocommunications Authority. (2024a). *Magic valley*. https://english.nmhh.hu/child-protection/magic-valley

National Media and Infocommunications Authority. (2024b). *Gyerekaneten.hu*. https://english.nmhh.hu/child-protection/gyerekaneten

National Media and Infocommunications Authority. (2025a). *Annual activity report of the Hungarian Digital Services Coordinator 2024*. https://english.nmhh.hu/

National Media and Infocommunications Authority. (2025b, December 15). *Filtered internet service available from mobile operators starting in January*. https://english.nmhh.hu/

National Media and Infocommunications Authority. (2026a, April 15). *Stark differences in the digital education of Hungarian families*. https://english.nmhh.hu/

National Media and Infocommunications Authority. (2026b). *Internet hotline*. https://english.nmhh.hu/internethotline-intro

National Media and Infocommunications Authority. (2026c). *The NMHH's media-related tasks and powers*. https://english.nmhh.hu/media_activity

National Media and Infocommunications Authority. (2026d, May 12). *Online abuse still mostly committed against children in 2025*. https://english.nmhh.hu/

National Media and Infocommunications Authority. (2026e). *Media Market Report 2025: Digital parenting strategies*. https://english.nmhh.hu/

National Media and Infocommunications Authority. (2026f, March 31). *Hungarian pre-schoolers in digital trap?* https://english.nmhh.hu/

National Media and Infocommunications Authority. (2026g, February 16). *The child as a brand*. https://english.nmhh.hu/

Nicolai, S., Rui, T. (Y.), Zubairi, A., Seluget, C., & Kamninga, T. (2023). *EdTech and parental engagement*. Paper commissioned for the 2023 Global Education Monitoring Report, Technology in Education. UNESCO.

Nigeria Data Protection Commission. (2025). *General Application and Implementation Directive (GAID) 2025*. https://ndpc.gov.ng/

Nigerian Communications Commission. (2024a). *Child online protection: Young children and digital technology* (Final report). https://ncc.gov.ng/

Nigerian Communications Commission. (2024b). *Parenting 101 for digital citizens*. NCC.

Nigerian Communications Commission. (2025). *Keeping children safe online*. NCC Consumer Affairs Bureau.

Nigerian Communications Commission. (2026a). *Internet code of practice 2026*. https://ncc.gov.ng/

Nigerian Communications Commission. (2026b). *Guidance notes on the Internet Code of Practice 2026*. https://ncc.gov.ng/

Nishma Bharadia. (2026). *Individualism vs. the benefits of community: Rediscovering the village*. https://nishmabharadia.com/individualism-vs-the-benefits-of-community

OECD. (2021). *Children in the digital environment: Revised typology of risks*. OECD Digital Economy Papers, No. 302. OECD Publishing. https://doi.org/10.1787/9b8f222e-en

OECD. (2021a). *OECD digital education outlook 2021: Pushing the frontiers with AI, blockchain and robots*. OECD Publishing. https://doi.org/10.1787/589b283f-en

OECD. (2021b). *Digital security risk management: Principles and policy approaches*. OECD Publishing.

OECD. (2021c). *Education and awareness approaches to digital security risk management*. OECD Publishing.

OECD. (2021d). Measuring what matters for child well-being and policies. OECD Publishing.

OECD. (2022). *Companion document to the OECD Recommendation on Children in the digital environment*. OECD Publishing. https://doi.org/10.1787/a2ebec7c-en

OECD. (2024). *Towards digital safety by design for children*. OECD Publishing. https://doi.org/10.1787/c167b650-en

OECD. (2025). *From playgrounds to platforms – childhood in the digital age*. OECD Policy Insights on Well-being, Inclusion and Equal Opportunity, No. 18. OECD Publishing. https://doi.org/10.1787/a2c18146-en

OECD. (2025). *How's life for children in the digital age?* OECD Publishing.

OECD. (2026). *Privacy principles*. https://www.oecd.org/en/topics/privacy-principles.html

Office of the National Security Adviser. (2021). *National Cybersecurity Policy and Strategy 2021*. Federal Republic of Nigeria.

Ogilvy Malaysia (2025). *The Future of Parenting*. Ogilvy Research & Insight.

Organisation for Economic Co-operation and Development. (2011). *Doing better for families*. OECD Publishing. https://doi.org/10.1787/9789264098732-en

Organisation of Islamic Cooperation. (2020). *OIC Strategy for the Empowerment of the Marriage and Family Institution and Preservation of Its Values in the Muslim World (2020–2025)*. https://www.oic-oci.org/

Parenting for Wellness. (2026). *Parenting for wellness toolbox for parents*. https://parentingforwellness.hpb.gov.sg/

Personal Data Protection Council. (2025). *Data Protection Impact Assessment (DPIA) guideline*. https://www.modee.gov.jo/

Platform KID. (n.d.). *Tentang platform KID*. Retrieved June 24, 2026, from https://platformkid.my/tentang-kami/

Ponti, M. (2023). Screen time and preschool children: Promoting health and development in a digital world. *Paediatrics & Child Health, 28*(3), 184–192. https://doi.org/10.1093/pch/pxac125

Postman, N. (1992). *Technopoly: The surrender of culture to technology*. Vintage Books.

Presidency of Religious Affairs. (2026). *e-Diyanet mobile services*. https://mobilhizmetler.diyanet.gov.tr

Presidency of the Republic of Türkiye Digital Transformation Office. (2021). *National artificial intelligence strategy (2021–2025)*.

PWC. (n.d.). *AI in Nigeria – Opportunities, challenges and strategic pathways*. https://www.pwc.com/ng/en/assets/pdf/ai-in-nigeria-a.pdf

Radio and Television Supreme Council. (2026). *Çekirdek ailesi* [Video playlist]. YouTube. https://www.youtube.com/playlist?list=PLxpnv_CvC87aUgPPXWJQztl8ynC8fidUL

Radio and Television Supreme Council. (2026). *RTÜK Media and Children Magazine*. https://www.rtuk.gov.tr/rtuk-medya-ve-cocuk-dergisi-4443

Radio and Television Supreme Council. (2026). *Smart Signs: Protective symbol system*. https://www.rtukisaretler.gov.tr/content?id=1

Regulation on the provision of radio, television and on-demand broadcasting services via the Internet. (2019, August 1). *Official Gazette*. https://www.resmigazete.gov.tr/eskiler/2019/08/20190801-5.html

Regulations.ai. (2021). *Malaysia digital economy blueprint (MyDIGITAL)* (Record No. RAI-MY-NA-MDEBMXX-2021). Regulations.ai Regulatory Database. https://regulations.ai/regulations/RAI-MY-NA-MDEBMXX-2021

Safe Online. (2026). *Disrupting harm*. https://safeonline.global/disrupting-harm-2/

Save the Children Jordan. (2024). *Behind the screens: Safety in digital spaces for children aged 10–17 in Jordan*. https://resourcecentre.savethechildren.net/

Save the Children Jordan. (2025). *Safer Internet Day: Prevention and awareness key elements for protecting children online*. https://savethechildren.org.jo/

Senate of the Federal Republic of Nigeria. (2026, July 7). *Order Paper: First reading of the Child Online Access Protection Bill*. National Assembly of Nigeria.

SESRIC. (2017). *Safeguarding family values and the institution of marriage in OIC countries*. SESRIC.

SESRIC. (2023). *Marriage and family institution in OIC member countries*. SESRIC.

SESRIC. (2024). *Statistical yearbook on OIC member countries 2024*. SESRIC.

Serevan, B. (2025). Al-Ghazali's principle of trust (Amanah) as a framework for ethical AI governance in organizations. AI and Ethics, 5(5), 5273–5282. https://doi.org/10.1007/s43681-025-00780

Shawareb, I. J., Alnasraween, M. S., Al Qasas, M. K., & Abduldaim, G. E. (2025). The role of parents in achieving digital security for kindergarten children in Jordan and Saudi Arabia. *Educational Process: International Journal, 18*, e2025476. https://doi.org/10.22521/edupij.2025.18.476

Shi, X., He, J., & Niu, G. (2024). The association between family socioeconomic status and children's digital literacy: The explanatory role of parental mediation. *Adolescents, 4*(3), 386–395. https://doi.org/10.3390/adolescents4030027

Siliutina, I., Tytar, O., Barbash, M., Petrenko, N., & Yepyk, L. (2024). Cultural preservation and digital heritage: Challenges and opportunities. *Amazonia Investiga, 13*(75), 262–273. https://doi.org/10.34069/AI/2024.75.03.22

Singh, P. (2021). Reverse socialization. In G. Ritzer (Ed.), *The Blackwell encyclopedia of sociology*. https://doi.org/10.1002/9781405165518.wbeos1805

SNOWFLAKE. (2026). *Data governance models: Comparing centralized, decentralized and federated approaches*. https://www.snowflake.com/en/data-governance/models/

Soyoof, A., Reynolds, B. L., Neumann, M., Scull, J., Tour, E., & McLay, K. (2024). *The impact of parent mediation on young children's home digital literacy practices and learning: A narrative review*. Journal of Computer Assisted Learning, 40(1), 65–88.

Srinuan, C., & Bohlin, E. (2011). *Understanding the digital divide: A literature survey and ways forward*. Paper presented at the 22nd European Regional Conference of the International Telecommunications Society (ITS2011), Budapest, Hungary.

STATISTA. (2025). *Number of internet users in Africa as of October 2025*. https://www.statista.com/

Statista Research Department. (2024). *Internet usage in Malaysia: Statistics & facts*. Statista. https://www.statista.com/topics/11756/internet-usage-in-malaysia/

Steinberg, S. B. (2017). Sharenting: Children's privacy in the age of social media. *Emory Law Journal, 66*(4), 839–884.

Süveges-Heilingbrunner, K. (2024). *Digital Decade Report: Hungary's broadband coverage above average, but efforts in key areas should be stepped up*. https://digital-skills-jobs.europa.eu/

Taipale, S. (2019). *Intergenerational connections in digital families*. Springer. https://doi.org/10.1007/978-3-030-11947-8_2

Takhshid, Z. (2023). Children's digital privacy and the case against parental consent. *Texas Law Review, 101*(6), 1417–1455.

Tan, C. Y., Xu, N., Liang, M., & Li, L. (2025). Meta-analysis of associations between digital parenting and children's digital well-being. *Educational Research Review, 48*, 100699. https://doi.org/10.1016/j.edurev.2025.100699

Tan, C. Y., Pan, Q., Tao, S., Liang, Q., Lan, M., Feng, S., Cheung, H. S., & Liu, D. (2024). Conceptualization, measurement, predictors, outcomes, and interventions in digital parenting research: A comprehensive umbrella review. Educational Research Review, 45, 100647

Tech Herfrica. (2026). *Nigeria aims for 70% digital literacy by 2027 despite 63.1% current rate*. https://www.techherfrica.org/

Telecommunications Regulatory Commission. (2026, February 11). *Cabinet approves formation of a national committee to protect children and adolescents from risks associated with social media and Internet use*. https://www.trc.gov.jo/

Telecommunications Regulatory Commission. (n.d.). *About the commission*. https://trc.gov.jo/EN/Pages/About_the_Commission

Telenor Asia. (2024). *Digital lives decoded 2024: Malaysia*.

Török, L. (2024). Digital transformation of Hungary's economy between 2015 and 2021: Results and future objectives. *Sustainability, 16*(11), 4684. https://doi.org/10.3390/su16114684

Tóth, J., & Kardosné Kaponyi, E. (2024). Homo digitalis in the EU and in Hungary. *Pécs Journal of International and European Law, I*, 48–70. https://doi.org/10.15170/PJIEL.2024.1.4

Tullis, C. B. (2025). *Jordan digital public infrastructure diagnostic*. World Bank. https://doi.org/10.1596/42812

Tunç, C., Akkaş, H., & Bayhan Karapınar, P. (2020). The mediating effect of work–family conflict in the relationship between smartphone use and employee well-being. *Journal of Organizational Behavior Review, 2*(1), 31–48. https://izlik.org/JA23DB54DK

Türkiye Green Crescent Society. (2026). *Türkiye addiction prevention training programs*. https://tbm.org.tr

Türkiye Radio and Television Corporation. (2026). *TRT Çocuk Library*. https://www.trtcocuk.net.tr/trt-cocuk-kitaplik

Türkiye Radio and Television Corporation. (2026). *TRT Çocuk Parent Academy*. https://ebeveynakademisi.trtcocuk.net.tr

Türkiye Statistical Institute. (2024). *Information and communication technologies usage survey among children*. TÜİK.

Türkiye Statistical Institute. (2025). *Household information and communication technologies usage survey*. TÜİK.

Türkiye Statistical Institute. (2026, February 9). *Results of the address-based population registration system, 2025* (News Bulletin No. 53899). TÜİK Data Portal.

Turkle, S. (2006). Relational artifacts with children and elders: The complexities of cybercompanionship. *Connection Science, 18*(4), 347–361. https://doi.org/10.1080/09540090600868912

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*. Basic Books.

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.

UNESCO. (2026). *Albania digital education project*. https://media.unesco.org/

UNFPA. (2025). *Nigeria population 2025*. United Nations Population Fund. https://www.unfpa.org/data/world-population/NG

UNICEF. (2017). *The state of the world's children 2017: Children in a digital world.* https://www.unicef.org/reports/state-worlds-children-2017

UNICEF. (2020a). *Adolescent engagement and skills acquisition in digital spaces: East Asia and Pacific regional report.* UNICEF East Asia and Pacific Regional Office.

UNICEF. (2020b). *What works to prevent online and offline child sexual exploitation and abuse: Review of national education strategies in East Asia and the Pacific.* United Nations Children's Fund.

UNICEF Jordan. (2021). *Cyberbullying: What is it and how to stop it.* https://www.unicef.org/jordan/

UNICEF Kazakhstan. (2024, February 6). *The 'CYBER TUMAR' informational and educational campaign launched in Kazakhstan: Protect children online.* https://www.unicef.org/kazakhstan/

UNICEF Kazakhstan. (2025). *Protecting children from online violence, abuse and exploitation in Kazakhstan.* https://www.unicef.org/kazakhstan/

UNICEF Nigeria. (2025). *Annual report 2024.* UNICEF.

UNICEF Nigeria. (n.d.). *Protecting children in the digital world: A guide for parents, caregivers and children.* UNICEF.

UNICEF Innocenti – Global Office of Research and Foresight. (2025). Childhood in a digital world: Screen time, digital skills and mental health. UNICEF Innocenti.

UNICEF Office of Strategy and Evidence – Innocenti. (2026). *Snapshot of AI usage and concerns among children and parents: Insights from 10 countries.* https://www.unicef.org/innocenti/

United Nations, Department of Economic and Social Affairs, Population Division. (2024). *World Population Prospects 2024.* https://population.un.org/wpp/

Uteno, I. M., Mtsea, T. T., & Chinyere, E. J. (2025). Digital education in Nigeria: Challenges and solutions. *European Journal of Business Startups and Open Society, 5*(11), 32–39.

Virtue, T., & Rainey, J. (2015). Information governance and risk management. In *HCISPP Study Guide* (pp. 91–130). Elsevier. https://doi.org/10.1016/C2013-0-14277-8

Walker, S. K. (2021). *Technology use and families: Implications for work-family balance and parenting education.* UN D.E.S.A., Division for Inclusive Social Development.

WAM. (2020). *Launch of the digital quality of life protection hotline.* https://www.wam.ae/

We are Social. (2025). *Digital 2026 global overview report.* https://wearesocial.com/me/blog/2025/10/digital-2026-global-overview-report/

We Are Social & Meltwater. (2025). *Digital 2025: Türkiye report.*

Weldali, M. (2026, January 28). 96.5% of Jordanian households connected to Internet — data. *The Jordan Times.* https://jordantimes.com/news/local/965-of-jordanian-households-connected-to-internet-data

Winner, L. (1980). Do artifacts have politics? *Daedalus, 109*(1), 121–136.

World Bank. (2016). *World development report 2016: Digital dividends.* https://www.worldbank.org/en/publication/wdr2016

World Bank. (2024a). *Jordan: The SANAD portal for digital government services-citizen-centric public services that are universally accessible.* https://doi.org/10.1596/41110

World Bank. (2024b). *World Bank GovTech operations in Jordan: A digital transformation case study.* https://documents1.worldbank.org/

World Bank. (2025a). *Jordan country overview.* https://www.worldbank.org/ext/en/country/jordan

World Bank. (2025b). *Resettlement policy framework: Building Resilient Digital Infrastructure for Growth (BRIDGE) report.* World Bank Group.

World Bank. (2026). *Implementation status & results report: Jordan People-Centric Digital Government Program for results (P180291).* https://documents.worldbank.org/

World Health Organization, United Nations Children's Fund, & World Bank Group. (2018). *Nurturing care for early childhood development: A framework for helping children survive and thrive to transform health and human potential.* World Health Organization. https://www.who.int/publications/i/item/9789241514064

Yürekli, M. (2022, June 22). Sosyal medyanin aile üzerindeki etkisi: Dijital aile. *Haber7com*. https://www.haber7.com/yazarlar/mustafa-yurekli/3234916-sosyal-medyanin-aile-uzerindeki-etkisi-dijital-aile

Zehir, B., & Odabaşı, H.F. (2025). Digital transformation in Central Asia: Opportunities and risks in a late start. *Digital Security & Media,* 2(1), 3–15. https://izlik.org/JA46MS46CN

Zgambo, M., Anyango, E., Arabiat, D. H., Ngune, I., Mörelius, E., Zhang, M., & Whitehead, L. C. (2025). Effect of digital safety interventions on parental practices in safeguarding children's digital activities: Systematic review and meta-analysis. JMIR Pediatrics and Parenting, 8, e70745.





COMCEC