

The Gambia's National Child and Vulnerable Groups Online Protection Policy

Country: The Republic of The Gambia

Project Name: Western Africa Regional Digital Integration Program

Project ID: 176932

Contract Ref: WARDIP/C3.7/2024/ IC-IND007

Submitted By:

Prof. Salma Abbasi, PhD, FRGS, FCMI, FRSA
Chairperson and CEO, eWorldwide Group (eWWG)

Tel: +44 780 327 9000

Email: salma@e-wwg.com



October, 2024

Table of Contents

Executive Summary	iv
Abbreviations and Acronyms	vi
1.0 Introduction and Background	1
1.1 Global Trends on Current and Emerging Online Risks and Harms	1
1.2	3
1.2.1 Content Risks.....	3
1.2.2 Contact Risks.....	4
1.2.3 Conduct Risks.....	5
1.2.4 Contract Risks.....	5
1.3 The Gambian Context	6
2.0 International and Regional Frameworks and Government Commitments	8
2.1 Online Protection of Children	8
2.2 Online Protection of Women	9
2.3 Online Protection of Persons with Disabilities.....	9
2.4 Online Protection of Older Persons.....	10
3.0 Guiding Principles	11
3.1 Child and Human Rights-based	11
3.2 Address all Forms of Online Risk.....	11
3.3 Holistic.....	11
3.4 Inclusive.....	11
3.5 Multi-sectoral	12
3.6 Regional and Global Collaboration	12
3.7 Participation of Children and Vulnerable Groups.....	12
4.0 Policy Objectives	12
5.0 Vision and Mission	12
6.0 Policy Pillars for Child and Vulnerable Groups Online Protection in The Gambia	13
6.1 Enhance Governance.....	13
6.2 Build Institutional Capacity	13
6.3 Review and Reform Legal and Regulatory Frameworks	14
6.4 Strengthen Response and Support Systems.....	14
6.5 Engage Digital Service Providers.....	15
6.5.1 Internet Service Providers	15
6.5.2 GSM Operators.....	16
6.5.3 Content Developers	16

6.6	Improve Training for Law Enforcement, Judiciary and Social Service.....	16
6.7	Incorporate Online Safety in Education.....	17
6.8	Raise Public Awareness on Online Safety.....	17
6.9	Promote Research and Development.....	18
6.10	Enhance International Cooperation.....	18
6.11	Integrate Child and Vulnerable Groups Online Protection in Emergencies and Pandemics.....	18
7.0	Institutional Framework for Implementation	19
8.0	Monitoring and Evaluation Framework	22

Executive Summary

While the digital environment offers significant benefits for children and vulnerable groups, including women, persons with disabilities and older person, it also exposes them to increasingly serious and complex online risks and harms such as disinformation and misinformation, online grooming, cyberbullying and data exploitation. Global trends, including the rapid evolution of artificial intelligence, have exacerbated these risks and harms, making it imperative for The Gambia to adopt protective measures.

The Gambia's National Child and Vulnerable Groups Online Protection Policy is a comprehensive framework designed to safeguard children and vulnerable groups from the rising risks and harms present in the digital world. The policy is led by the Ministry of Communications and Digital Economy and developed through a multi-stakeholder approach with support from the World Bank. The policy aligns with The Gambia's National Cybersecurity Policy of The Gambia 2022–2026, the National Cybersecurity Strategy and Action Plan of The Gambia 2022–2026, and the Digital Transformation Strategy 2023–2028.

The Gambia's National Child and Vulnerable Groups Online Protection Policy is also well aligned with many international and regional frameworks, including the United Nations Convention on the Rights of the Child, the International Telecommunication Union's Guidelines for Policymakers on Child Online Protection, and the African Union's Child Online Safety and Empowerment Policy, among other international and regional standards. The Gambia's commitment to these frameworks underscores its dedication to protecting all children and vulnerable groups from online risks and harms.

The vision of The Gambia's National Child and Vulnerable Groups Online Protection Policy is to ensure a safe, secure and supportive digital environment for all children and vulnerable groups in The Gambia. The mission is to establish and implement a comprehensive online protection framework that leverages global best practices and multi-stakeholder cooperation.

The Gambia's National Child and Vulnerable Groups Online Protection Policy is structured around 11 key pillars with policy actions that aim to:

1. Enhance governance through coordinated leadership and a multi-sector stakeholder committee.
2. Build institutional capacity to implement, monitor and evaluate online safety measures.
3. Review and reform legal and regulatory frameworks to address online risks in line with international and regional standards.
4. Strengthen response and support systems, ensuring that law enforcement, judicial systems and social services have the capacity to address all forms of online risks and harms that children and vulnerable groups are exposed to.
5. Engage digital service providers, including internet service providers, global system for mobile communication (GSM) operators and content developers, to establish robust online safety guidelines.
6. Improve training for law enforcement, the judiciary and social services.
7. Incorporate online safety into education, focusing on digital literacy.
8. Raise public awareness about online safety, especially among children, vulnerable groups, parents and caregivers.
9. Promote research and data collection to inform policy implementation and improvement.

10. Enhance international cooperation for joint investments and knowledge sharing.
11. Integrate child and vulnerable groups online protection in emergencies and pandemics.

The Gambia's National Child and Vulnerable Groups Online Protection Policy marks a significant step forward in ensuring that The Gambia's digital transformation is inclusive, secure and protective of its most vulnerable populations.

Abbreviations and Acronyms

AI	Artificial Intelligence
ACRWC	African Charter on the Rights and Welfare of the Child
CEDAW	Convention on the Elimination of All Forms of Discrimination Against Women
CRPD	Convention on the Rights of Persons with Disabilities
ECOWAS	Economic Community of West African States
GSM	Global System for Mobile Communication
ICT	Information and Communications Technology
ITU	International Telecommunication Union
MOCDE	Ministry of Communications and Digital Economy
UNCRC	United Nations Convention on the Rights of the Child
UNICEF	United Nations Children's Fund

1.0 Introduction and Background

The Gambia's National Child and Vulnerable Groups Online Protection Policy has been developed in line with the National Cybersecurity Policy of The Gambia 2022–2026 and the National Cybersecurity Strategy and Action Plan of The Gambia 2022–2026 that have the protection of children and vulnerable groups as a strategic goal. The vulnerable groups include women, persons with disabilities and older persons. The development of this policy is led by the Ministry of Communications and Digital Economy (MOCDE), with support from the World Bank, through the Western Africa Regional Digital Integration Program.

The policy adopts a holistic, multi-stakeholder participatory approach, bringing together multi-sector stakeholders to develop holistic prevention and response to the online risks and harms that children and vulnerable groups are exposed to. The process of developing this policy involved a situational analysis that included research on the online risks and harms that children and vulnerable groups face, a review and analysis of legal and policy instruments and global best practices in addressing the online risks and harms, and an analysis of the opportunities and gaps in The Gambia regarding the online protection of children and vulnerable groups. In order to ensure that the policy is robust and inclusive, consultative workshops, roundtable discussions, seminars and an online questionnaire survey were conducted to obtain insights and perceptions from stakeholders across government, the private sector and civil society engaged in the online protection of children and vulnerable groups in The Gambia. In addition, the draft policy was presented at a validation workshop and shared with relevant stakeholders for comments and feedback.

The Gambia's National Child and Vulnerable Groups Online Protection Policy is based on world-class child online protection policies, strategies and guidelines. The policy aims to provide a common vision and understanding of what child and vulnerable groups online protection entails in The Gambia, ensuring a unified approach for greater and accelerated impact toward ensuring that the rights of every individual are met in the digital environment.

1.1 Global Trends on Current and Emerging Online Risks and Harms

The digital environment has become an integral part of everyday lives and interactions. The COVID-19 pandemic has propelled the shift of many activities into the digital world. As a result, children and vulnerable groups are spending more time online. Although digital platforms, tools and content open up numerous benefits and opportunities for learning, support and socializing, children and vulnerable groups are also being exposed to a wide spectrum of online risks and harms that are evolving at a rapid pace and becoming more serious and complex.

The 2023 Child Online Safety Index found that nearly 70% of children aged 8–18 worldwide have experienced at least one cyber risk incident in the past year.¹ A global survey of nearly 5,000 parents across nine countries showed that parents broadly share the same concerns regarding their children's online behaviors regardless of geographical location, suggesting that children across the globe are being exposed to similar online risks and harms.²

Similarly, for other vulnerable groups such as women, persons with disabilities and older persons, digital technologies offer numerous benefits, enabling access to online and mobile learning and digital health applications, increasing employment opportunities and engagement in e-commerce,

¹ DQ Institute, "2023 Child Online Safety Index," <https://www.dqinstitute.org/impact-measure/>.

² ITU, "Safeguarding Children Online: A service-specific view on risks and parental attitudes," October 2023, <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/Evidence-based-research.aspx>.

and promoting participation in online forums to voice their view and concerns. Yet, vulnerable groups' exposure to online risks and harms prevent them from fully leveraging the potential of digital technologies. For instance, global studies show that between 16% and 58% of women have experienced technology-facilitated gender-based violence.³ A global study found that in Africa, up to 90% of women have experienced or witnessed online and technology-facilitated violence.⁴ This form of violence not only results in physical and mental harms, but also silences women in online spaces and diminishes their engagement in economic, social and political domains.

The international community has classified the wide spectrum of online risks and harms into four broad categories – content, contact, conduct and contract.⁵ Across these four categories, there is increasing recognition of the risks from the use of artificial intelligence (AI) technologies that need to be prevented and mitigated. This classification of online risks has been adopted in the African Union Child Online Safety and Empowerment Policy 2024.⁶

The following provides a glimpse of current and emerging online risks and harms across the four categories, which are further discussed in Section 1.2:

- **Content** – Children and vulnerable groups are being exposed to inappropriate, potentially dangerous and illegal content online either by scrolling their social media feeds, or are sent by family members, peers or strangers. The types of content include child sexual abuse material, pornography, disinformation and misinformation, hate speech, and content that promote self-harm and violence. Generative AI tools are being used to rapidly create and spread such harmful content online, amplifying the harms experienced by children and vulnerable groups.
- **Contact** – Interacting with individuals, especially on social media networks, instant messaging apps and online gaming platforms, can expose children and vulnerable groups to contact risks and harms, such as online grooming, sextortion and radicalization. Generative AI technology is being used to create realistic deepfake sexual abuse images and videos based on real victims and used for sextortion. Violent extremists are also using AI to rapidly create and spread extremist content online, and develop chatbots that encourage children and vulnerable groups to join extremist groups.
- **Conduct** – The way that children and vulnerable groups use the internet may put them at risk. This includes the types of content that children and vulnerable groups create and share with their peers. The risks include cyberbullying and the non-consensual sharing of self-generated sexual content. AI-powered tools can be used to generate and automatically send large volumes of hateful and abusive messages targeted at the victims. AI can also be used to tailor harassments to individuals' vulnerabilities and interests, making them more damaging and harmful. In addition, AI can be used to rapidly spread false rumors and accusations to turn peers against the victims, leading to their social ostracism and isolation.
- **Contract** – Social media and online gaming platforms collect massive amounts of data on users' profile and their engagements on the platforms. Generally, they collect and process the data of children in the same way as they do for adults' data, unless they need to meet

³ UN Women, "FAQs: Trolling, stalking, doxing and other forms of violence against women in the digital age," <https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/tech-facilitated-gender-based-violence>.

⁴ Economist Intelligence Unit, "Measuring the Prevalence of Online Violence against Women," 2021, <https://onlineviolencewomen.eiu.com>.

⁵ Organisation for Economic Co-operation and Development, "Children in the Digital Environment: Revised Typology of Risks," January 2021, https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en.

⁶ African Union, "The African Union Child Online Safety and Empowerment Policy," 2024, https://au.int/sites/default/files/documents/43798-doc-African_Union_Child_Online_Safety_and_Empowerment_Policy_Feb_2024.pdf.

regulatory requirements. AI-driven algorithms can analyze online behavior based on the data collected to deliver targeted advertising, often exploiting the vulnerabilities of children and marginalized groups. This can lead to manipulation or exposure to inappropriate content. Moreover, AI models can perpetuate existing biases, leading to discriminatory practices that harm children and vulnerable groups. This can affect their access to resources, support and protection.

1.2 Impact of Online Risks and Harms on Children and Vulnerable Groups

An overview of the major content, contact, conduct and contract risks and their impact on children and vulnerable groups is discussed below.

1.2.1 Content Risks

Illegal and harmful content are affecting children and vulnerable groups' health and well-being, and contributing to self-harm and violence. One study shows 90% of boys and 60% of girls being exposed to pornography online before the age of 18, with boys seeing pornography by the age of 12, on average.⁷ Children's early exposure to pornography, especially those involving sexual violence, has been linked to low self-esteem among young people and harmful views of sex and relationships.⁸ Constant exposure to sexual and violent content can lead to their normalization and the seeking of more extreme forms of such content, as well as contribute to online grooming toward the production of self-generated sexual content or the joining of violent extremist groups, respectively.

Findings from the latest global report show that the amount of child sexual abuse material online increased by 87% between 2019 and 2022, with over 32 million reports made in 2022.⁹ Alarming, there was a 60% increase in sexual content depicting pre-pubescent children (ages 7–10 years) between 2021 and 2022,¹⁰ and content on extreme child sexual abuse (i.e., child suffering, rape, bestiality, sadism) doubled since 2020, with newborn babies and toddlers among the victims of the most severe kinds of sexual abuse. This type of content accounted for 20% of all content analyzed by Internet Watch Foundation in 2022.¹¹ The production and distribution of child sexual abuse material online result in re-victimization and re-traumatization through re-sharing. The trauma on survivors of child abuse and exploitation can be lifelong with long-lasting effects on their physical and mental well-being.

Children and vulnerable groups' exposure to disinformation and misinformation is another serious concern. Disinformation and misinformation are often extreme and sensational, containing content that contribute to inciting stereotyping, blame, hate, crime and violence targeted at certain groups based on race, sexual orientation, religion, etc. The algorithms used by social media platforms to generate advertising profit have been known to amplify the spread of misleading and extremist content over factual information, making these "fake" news spread faster and further than ever before. According to research, at least 81 countries worldwide use social media to propagate political disinformation and misinformation, manipulate opinion, and undermine public

⁷ Global News, "Is enough being done to protect children from viewing pornography online," 28 October 2016, <https://globalnews.ca/news/3031576/is-enough-being-done-to-protect-children-from-viewing-porn-online/>.

⁸ Children's Commissioner for England, "Evidence on pornography's influence on harmful sexual behaviour among children," 9 May 2023, <https://www.childrenscommissioner.gov.uk/resource/pornography-and-harmful-sexual-behaviour/>.

⁹ WeProtect Global Alliance, "Global Threat Assessment 2023," October 2023, <https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf>.

¹⁰ ICMEC, "Child Sexual Abuse Material: Model Legislation & Global Review," 10th Edition, October 2023, https://cdn.icmec.org/wp-content/uploads/2023/10/CSAM-Model-Legislation_10th-Ed-Oct-2023.pdf.

¹¹ Ibid.

trust in ways that can have severe adverse consequences on people's safety and well-being.¹² A majority (60%) of teachers surveyed by the United Nations Children's Fund (UNICEF) believe disinformation and misinformation are having a harmful effect on young people's well-being by increasing anxiety, damaging self-esteem and skewing their world view.¹³

1.2.2 Contact Risks

As individuals spend more time online on social media and online gaming platforms, sex offenders, traffickers and criminal groups have increased access to children and vulnerable groups through these platforms. Experts have issued warnings that social media and online gaming platforms are being targeted for recruitment by criminal groups.¹⁴ Once initial contacts are established, conversations can move to private messaging platforms where online grooming often take place. A study found that conversations with children on online gaming platforms can escalate into high-risk grooming situations within 19 seconds, with an average grooming time of just 45 minutes.¹⁵ Online gaming environments that facilitate adult-child intermingling, exchanging of virtual gifts and public ranking systems significantly increase online grooming risks.

Reports are showing rising incidences of sextortion, with increasing cases targeting younger children, both boys and girls.¹⁶ Sextortion refers to a type of exploitation whereby the perpetrator threatens to expose or share a sexual image or video to blackmail the victim into doing something, such as sharing more images and videos, paying money and/or engaging in sexual activity. Globally, reports of sextortion jumped from 139 in 2021 to over 10,000 in 2022, with their motivation shifting from sexual gratification to financial gains.¹⁷ Boys are increasingly being targeted for financial sextortion with many extorters posing as young girls online and approaching boys aged between 15 and 17 years via social media.¹⁸ This phenomenon has resulted in a string of cases where children have tragically taken their own lives.¹⁹

Radicalization is the social and psychological process through which a person moves toward supporting or becoming involved in extremist ideologies. Over the past decade and especially during the COVID-19 pandemic, the radicalization efforts of extremist groups have occurred at greater speed and spanned wider reach through the internet, particularly through social media and instant messaging platforms.²⁰ A study provides evidence that online interaction alone is

¹² UNICEF, "Digital misinformation / disinformation and children," August 2021, <https://www.unicef.org/globalinsight/media/2096/file/UNICEF-Global-Insight-Digital-Mis-Disinformation-and-Children-2021.pdf>.

¹³ Ibid.

¹⁴ Ethan Shone, "County lines: gangs using social media and online gaming to recruit children with promises of cash and phones," National World, 1 March 2023, <https://www.nationalworld.com/news/crime/county-lines-social-media-online-gaming-recruitment-criminal-gangs-cash-phones-4046387>; Adriana Loya, "Video games being used to recruit smugglers in the Valley," 12 News, 30 January 2022, <https://www.12news.com/article/news/local/arizona/drug-cartels-using-online-video-games-to-recruit-border-smugglers-in-valley/75-18cdc410-fe27-4f1d-9710-fdb70a5b467c>.

¹⁵ WeProtect Global Alliance, "Global Threat Assessment 2023," October 2023, <https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf>.

¹⁶ Internet Watch Foundation, "'Exponential increase in cruelty' as sextortion scams hit younger victims," 23 August 2024, <https://www.iwf.org.uk/news-media/news/exponential-increase-in-cruelty-as-sex-tortion-scams-hit-younger-victims/>.

¹⁷ ICMEC, "Child Sexual Abuse Material: Model Legislation & Global Review," 10th Edition, October 2023, https://cdn.icmec.org/wp-content/uploads/2023/10/CSAM-Model-Legislation_10th-Ed-Oct-2023.pdf.

¹⁸ WeProtect Global Alliance, "Global Threat Assessment 2023," October 2023, <https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf>.

¹⁹ South Wales Police, "'Epidemic' of sextortion cases targeting children sees National Crime Agency issue warning," 1 May 2024, <https://www.south-wales.police.uk/news/south-wales/news/2024/april/epidemic-of-sex-tortion-cases-targeting-children-sees-national-crime-agency-issue-warning/>; Libby Brooks, "'It can happen to any child': parents of sextortion victim send out warning," The Guardian, 29 April 2024, <https://www.theguardian.com/society/2024/apr/29/it-can-happen-to-any-child-parents-of-sex-tortion-victim-fight-for-justice>; Luke Barr, "Parents of teenager who died by suicide after sextortion scam urge 'tough' conversations with children," ABC News, 4 May 2023, <https://abcnews.go.com/US/parents-teenager-died-by-suicide-after-sex-tortion-scam-urge/story?id=99047305>.

²⁰ Jens F. Binder and Jonathan Kenyon, "Terrorism and the internet: How dangerous is online radicalization?" Frontiers in Psychology, 13 October 2022, <https://www.frontiersin.org/articles/10.3389/fpsyg.2022.997390/full>.

enough to recruit a vulnerable person into an extremist or terrorist group.²¹ Particularly on social media platforms, their newsfeed algorithm that feeds users tailored content on the platform has created echo chambers that amplify extremist voices and suppress any contrary opinions.²² Violent extremist groups are also making use of online games to spread propaganda and groom young people into joining them.²³ A United Nations study found that extremist groups are taking advantage of the popularity and attractiveness of gaming spaces among young people, and the ease of access and lack of moderation in those spaces to influence, manipulate and exploit young people.²⁴

1.2.3 Conduct Risks

Cyberbullying and online harassment have become well-recognized as severe public health issues affecting the mental and physical well-being of children and vulnerable groups.²⁵ According to a global survey conducted by UNICEF, one in three young people has been a victim of cyberbullying,²⁶ and evidence points to increasing rates of cyberbullying worldwide.²⁷ Cyberbullying may be contributing to increase in youth suicides. One 2018 study found that young adults under the age of 25 who were victimized by cyberbullying were twice as likely to commit suicide or self-harm in other ways.²⁸ Young people are also skipping school because of threats associated with cyberbullying.²⁹

Self-generated sexual content is sexually-explicit content (text, images and videos) created and shared by an individual, either voluntarily or are coerced into doing so. A 360% increase in self-generated sexual imagery of 7–10-year-olds from 2020 to 2022 has been reported to be circulating online.³⁰ While the sharing of sexual content between two consenting individuals is not a harm, there are rising incidences of self-generated sexual material being shared against individuals' wishes with the intent to harm. Children and vulnerable groups may also be coerced into producing sexual material through online grooming or in exchange for payment. Such incidences make them vulnerable to becoming victims of sextortion, cyberbullying and having their images used in child sexual abuse material collections. The content can quickly spread and remain in the digital environment permanently, which can lead to long-lasting physical and psychological harm on the targeted children and vulnerable groups. The stigma associated with

²¹ Anne Speckhard and Molly Ellenberg, "Is Internet Recruitment Enough to Seduce a Vulnerable Individual into Terrorism?" International Center for the Study of Violent Extremism, 19 April 2020, <https://www.icsve.org/is-internet-recruitment-enough-to-seduce-a-vulnerable-individual-into-terrorism/>.

²² Alexander Meleagrou-Hitchens and Nick Kaderbhai, *Research Perspectives on Online Radicalisation: A Literature Review 2006-2016* (VOX-Pol Network of Excellence, 2017), <https://icsr.info/2017/05/03/icsr-vox-pol-paper-research-perspectives-online-radicalisation-literature-review-2006-2016-2/>.

²³ Sara Zeiger and Joseph Gyte, "Prevention of Radicalization on Social Media and the Internet," in *Handbook of Terrorism Prevention and Preparedness*, International Centre for Counter-Terrorism, 2023, https://www.icct.nl/sites/default/files/2023-01/Chapter-12-Handbook_0.pdf.

²⁴ United Nations Office of Counter-Terrorism, "Examining the Intersection Between Gaming and Violent Extremism," 2022, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_research_launch_on_gaming_ve.pdf.

²⁵ Chengyan Zhu et al., "Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures," *Frontiers in Public Health*, 11 March 2021, <https://www.frontiersin.org/articles/10.3389/fpubh.2021.634909/full>.

²⁶ UNICEF, "UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying," Press Release, 3 September 2019, <https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying>.

²⁷ Sam Cook, "Cyberbullying facts and statistics for 2018 – 2022," Comparitech, 14 November 2022, <https://www.comparitech.com/internet-providers/cyberbullying-statistics/>.

²⁸ Ibid.

²⁹ UNICEF, "UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying," Press Release, 3 September 2019, <https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying>.

³⁰ WeProtect Global Alliance, "Global Threat Assessment 2023," October 2023, <https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf>.

self-generated sexual content can make it difficult for individuals to pursue educational opportunities or find employment.

1.2.4 Contract Risks

Social media and online gaming platforms are collecting and processing personal data of children and vulnerable groups, including geolocation, biometrics and other sensitive information, without genuine informed consent. This can result in commercial exploitation, targeted advertising and unlawful surveillance, and can expose children and vulnerable groups to illegal and age-inappropriate products and services, as well as potentially misleading or manipulative marketing strategies.

Concerns related to contract risks are not limited to social media and online gaming platforms, but also to mobile and online applications, including educational technology products used by children and vulnerable groups. A study found a majority of governments around the world endorsing educational technology products for use during the COVID-19 pandemic that handled children's personal data in ways that risked or infringed on their rights.³¹ Most of these products sent or granted access to children's data to advertising technology companies. In doing so, some educational technology products targeted children with behavioral advertising that not only distorted children's online experiences, but also risked influencing their opinions and beliefs.

As AI is being adopted globally and across all sectors, vast amounts of data are being collected from different sources to train the AI systems and make data-driven decisions about individuals, which can impact on individuals' rights in significant ways. For instance, banks are using AI to help decide loans, recruiters and employers are using AI to select job candidates, social workers are using AI to identify eligible beneficiaries for welfare subsidies, and the police and courts are using AI to determine whether one is a potential criminal or is likely to recommit a crime. As AI uses the data collected to assess and predict behavior, abilities and performances, they can limit children and vulnerable groups' opportunities and development, and affect their access to education, employment, healthcare and financial services. The biases in datasets and algorithms can potentially lead to discrimination against certain social groups and exacerbate inequalities.

A serious concern is the growing popularity of social chatbots powered by generative AI, such as Snapchat's My AI and Replika, which users can have personal and intimate conversations with 24/7. Research shows that children are much more likely than adults to treat chatbots as if they are human, and will disclose more about their own mental health to a friendly-looking robot than to an adult.³² Without ethical frameworks or emotions of their own, and designed to nudge and keep users hooked, these chatbots can reinforce negative thoughts and tendencies that are acted out in real life, with cases of the chatbots encouraging suicide and commitment of crime already being reported.³³

1.3 The Gambian Context

The Gambia has an estimated population of 2.42 million (2024), with 40.8% of the population aged 0–15 years, and 3.0% of the population aged 65 years and over³⁴ (this figure is expected

³¹ Human Rights Watch, "Governments Harm Children's Rights in Online Learning," 25 May 2022, <https://www.hrw.org/news/2022/05/25/governments-harm-childrens-rights-online-learning>.

³² University of Cambridge, "Research: AI Chatbots have shown they have an 'empathy gap' that children are likely to miss," 15 July 2024, <https://www.cam.ac.uk/research/news/ai-chatbots-have-shown-they-have-an-empathy-gap-that-children-are-likely-to-miss>.

³³ Kyle Chayka, "Your A.I. Companion Will Support You No Matter What," *The New Yorker*, 13 November 2023, <https://www.newyorker.com/culture/infinite-scroll/your-ai-companion-will-support-you-no-matter-what>.

³⁴ Gambia Bureau of Statistics, "The Gambia 2024 Population and Housing Census: Preliminary Report," August 2024.

to almost double to 5% by 2050).³⁵ According to the 2013 census, 1.2% of The Gambia's population have a disability.³⁶ The Gambia is a least developed country that is ranked 174 out of 191 countries in the 2024 Human Development Index, and the 2023 Multidimensional Poverty Index shows that 41.7% of the population are multidimensionally poor.

The Gambia is highly vulnerable to the impacts of climate change, including flooding, storm, droughts and coastal erosion, potentially resulting in significant economic and social losses, including worsening food insecurity and poverty, rising number of persons with disabilities, and deterioration in human capital. Today, The Gambia is still recovering from a range of shocks and crises arising from the COVID-19 pandemic, the subregional impact of the Ebola crisis, post-election electoral and political crisis, and erratic rainfall patterns. In 2022, The Gambia experienced the worst flooding in its history, affecting 95,609 people.

The Gambia is transitioning into a digital economy and society. It has passed the Information and Communications Technology Agency Act in 2019 that aims to encourage the optimum use of digital technology, and investment in the information and communications technology (ICT) infrastructure and digital services. Subsequently, the Digital Transformation Strategy 2023–2028 and the National Digital Economy Master Plan 2023–2033 were adopted to accelerate economic recovery and stimulate growth.

The Gambia has made significant progress in expanding access to mobile and internet services over the past two decades. The overall digital transformation of The Gambia is in the developing phase.³⁷ The Gambia ranks 120th out of 134 economies in the 2023 Network Readiness Index, and 174th out of 193 economies in the United Nations E-Government Development Index 2022, rising seven places following the prior survey conducted in 2020. The percentage of the population using the internet rose rapidly from 0.92% in 2000 to 54.2% in 2022,³⁸ which also means that a much larger proportion of the country's population is exposed to online risks and harms.

According to the latest International Telecommunication Union (ITU) Global Cybersecurity Index released in September 2024, The Gambia's relative strength is having legal and organizational measures for cybersecurity in place, while more effort is needed in strengthening technical, capacity development and cooperation measures to foster a culture of cybersecurity resilience (Figure 1).

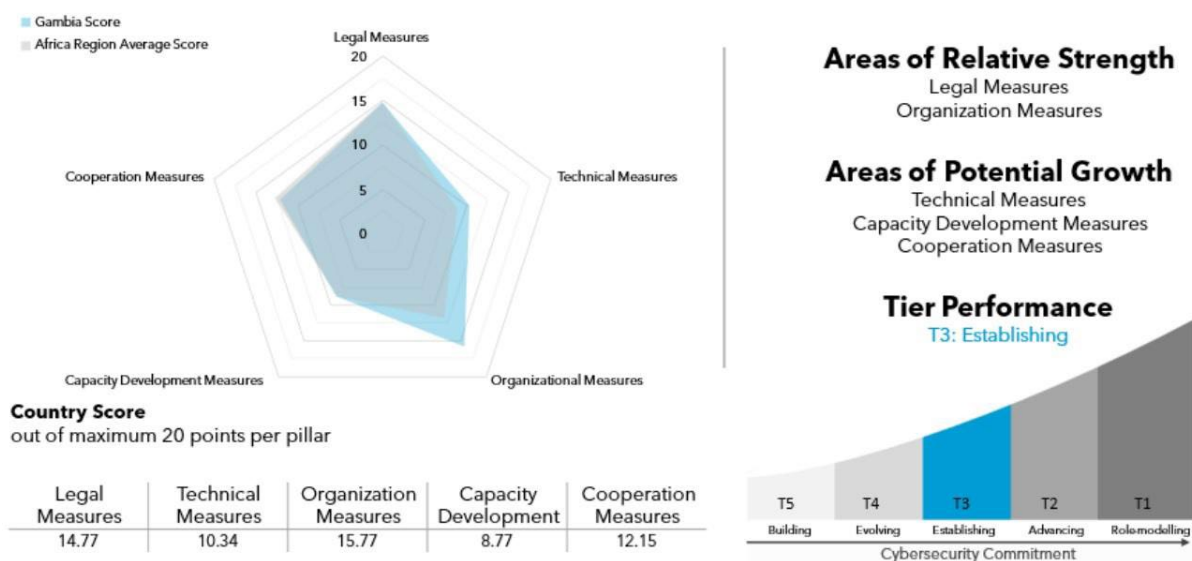
Figure 1: Summary of The Gambia's Performance in the ITU Global Cybersecurity Index 2024

³⁵ United Nations Department of Economic and Social Affairs, *World Population Ageing 2023: Challenges and Opportunities of Population Ageing in the Least Developed Countries* (New York, 2023).

³⁶ Those with physical disability constitute 23.7%, visual impairment at 16.6%, hearing at 16.7%, speaking 12.9% and strange behavior 8.0%. Source: United Nations Partnership on the Rights of Persons with Disabilities, "Situational Analysis of the Rights of Persons with Disabilities in The Gambia," 2021, https://unprpd.org/new/wp-content/uploads/2023/12/CR_Gambia_2021-9a7.pdf.

³⁷ MOCDE, Government of The Gambia, "National Digital Economy Master Plan 2023–2033," <https://mocde.gov.gm/wp-content/uploads/2023/10/Final-The-Gambia-Digital-Economy-Master-Plan-2023-20233.pdf>.

³⁸ ITU, "Data Hub: Gambia - Individuals using the Internet," <https://datahub.itu.int/data/?e=GMB&c=701&i=11624&v=chart>.



Source: ITU, *Global Cybersecurity Index 2024*, 5th Edition (Geneva, 2024), https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

This National Child and Vulnerable Groups Online Protection Policy brings together key stakeholders to coordinate, capacitate and accelerate impactful actions toward the online protection of all children and vulnerable groups in The Gambia.

2.0 International and Regional Frameworks and Government Commitments

The Gambia is a signatory to the 2010 Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection within ECOWAS and the Malabo Convention on Cybersecurity and Personal Data Protection in 2022. Subsequently, The Gambia has adopted the National Cybersecurity Policy of The Gambia 2022–2026 that has the protection of children and vulnerable groups as one of its strategic goals. The National Cybersecurity Strategy and Action Plan of The Gambia 2022–2026 includes actions to protect children and vulnerable groups online and ensure their online safety. Specifically, the actions include the following:

Actions for Objective 17: Ensure Online Safety for Vulnerable Groups, Especially Children

- Develop and disseminate online safety guidelines and best practices to protect vulnerable groups in The Gambia, especially children, from cyberthreats.
- Create and implement mechanism for child online protection by establishing a section under the National Cybersecurity Coordination Directorate to handle matters relating to child online exploitation and abuse.
- Deploy special awareness programs to target and inform children and other vulnerable groups about safe and responsible use of the internet.

Actions for Objective 18: Deploy Tools to Ensure Vulnerable Groups such as Children are Safe Online

- Promote the deployment of technical measures or web filtering tools that prevent access to harmful content by children and other vulnerable groups.
- Encourage internet service providers and other services providers to make their clients, especially parents and guardians aware of how to leverage available tools, technologies to manage potential risks to vulnerable groups while accessing services online.

Action for Objective 19: Passage of Cybercrime and Other Laws

- Ensure that a national child protection online legislation is enacted and implemented in accordance with international and regional standards.

The Gambia is strongly committed to the protection of children and other vulnerable groups, such as women, persons with disabilities and older persons, from all forms of online harm, exploitation and abuse, in line with international and regional frameworks.

2.1 Online Protection of Children

The United Nations Convention on the Rights of the Child (UNCRC) serves as the cornerstone of international child protection efforts, both online and offline. The UNCRC General Comment No. 25 (2021)³⁹ on children's rights in relation to the digital environment provides guidance on relevant legislative, policy and other measures to ensure compliance with obligations under the UNCRC and the Optional Protocol to the UNCRC on the Sale of Children, Child Prostitution and Child Pornography. The African Charter on the Rights and Welfare of the Child (ACRWC), based on the UNCRC, focuses on the protection of children from all forms of exploitation and abuse. The UNCRC was ratified by The Gambia on 3 August 1990, and the ACRWC was ratified by The Gambia on 14 December 2000. The Gambia's Children's Act 2005 (amended in 2016) is based on the CRC and ACRWC.

The ITU Guidelines for Policymakers on Child Online Protection is based on global standards and provides a flexible and adaptable framework for policymakers in ITU member states to develop their child online protection policy in line with national development policies and plans. These guidelines provide a holistic approach to respond to all potential risks and harms that children may encounter, and to building safe, age-appropriate, inclusive and participatory digital spaces for children. The Gambia is an ITU member state and The Gambia's National Child and Vulnerable Groups Online Protection Policy is well aligned with the ITU Guidelines for Policymakers on Child Online Protection.

In February 2024, the African Union Executive Council adopted the African Union Child Online Safety and Empowerment Policy,⁴⁰ which is based on the principles of the UNCRC General Comment No. 25 (2021). The policy aims to assist member states with the development of national child online safety and empowerment policies, paving the way for a safer and nurturing online environment for children. The Gambia's National Child and Vulnerable Groups Online Protection Policy is well aligned with the African Union Child Online Safety and Empowerment Policy.

³⁹ United Nations Committee on the Rights of the Child, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," March 2021, <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>.

⁴⁰ African Union, "African Union Child Online Safety and Empowerment Policy," February 2024, <https://au.int/en/documents/20240521/african-union-child-online-safety-and-empowerment-policy>.

2.2 Online Protection of Women

The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) represents the global framework for addressing gender-based discrimination and violence. The CEDAW Committee issued General Recommendation No. 35 (2017) that explicitly includes online and technology-facilitated violence as a new form of gender-based violence against women that is within the scope of CEDAW. CEDAW was ratified by The Gambia on 16 April 1993.

The Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa, commonly known as the Maputo Protocol, based on CEDAW, aims to advance and protect the rights of women in Africa, and contains specific provisions against various forms of violence. The Maputo Protocol was ratified by The Gambia on 25 May 2005. The Gambia's Women's Act 2010 (amended in 2015) is based on CEDAW and the Maputo Protocol, and The Gambia's National Gender Policy (2010–2020) is being updated.

In 2022, the African Union adopted the Resolution on the Protection of Women Against Digital Violence in Africa. The resolution recognizes the obligation of member states to develop the necessary measures aimed at the protection of women in the digital environment, including the adoption of legislative, policy, and other measures, awareness raising programs, and training for people working with vulnerable women and survivors of exploitation and abuse. The Gambia's National Child and Vulnerable Groups Online Protection Policy is well aligned with the African Union's Resolution on the Protection of Women Against Digital Violence in Africa.

2.3 Online Protection of Persons with Disabilities

The Convention on the Rights of Persons with Disabilities (CRPD) sets out the fundamental human rights of persons with disabilities. It serves as a catalyst in enabling a shift from viewing persons with disabilities as objects of charity, medical treatment and social protection toward viewing them as full and equal members of society, with human rights. The CRPD and its Optional Protocol was ratified by The Gambia on 7 July 2015. The Gambia's Persons with Disabilities Act 2021 is the first comprehensive legislation on disability rights in The Gambia, developed in line with the CRPD. It specifically addresses intersectional vulnerabilities with provisions on protecting the rights of women, children and older persons with disabilities.

2.4 Online Protection of Older Persons

There is currently no global convention specifically dedicated to protecting the rights of older persons that has been adopted by the United Nations, although there has been ongoing advocacy by various organizations and civil society groups for the development of a global convention on the rights of older persons. There is also no global framework focused on the online protection of older persons. However, The Gambia has demonstrated commitment to the protection of older persons in The Gambia National Social Protection Policy 2015–2025.

As The Gambia strives toward digital transformation of its economy and society, the development and implementation of this National Child and Vulnerable Groups Online Protection Policy signals The Gambia's foresight, leadership and commitment in ensuring that children and vulnerable groups are protected from harm, and collective efforts are being made to promote their growth and well-being. The Gambia's National Child and Vulnerable Groups Online Protection Policy paves the way for an inclusive and whole-of-society approach to online safety.

3.0 Guiding Principles

The Gambia's National Child and Vulnerable Groups Online Protection Policy will be guided by the principles below.

3.1 Child and Human Rights-based

This policy aims to achieve a balance in respecting the full range of rights of children, women, persons with disabilities and older persons, as enshrined in international human rights law. It promotes individuals' access to the internet and respects and ensures their rights to freedom of expression, privacy and access to information, while at the same time, recognizes their rights to protection from all forms of risks and harms online.

3.2. Address all Forms of Online Risk

The policy aims to comprehensively address the wide spectrum of online risks and harms, including content, contact, conduct and contract risks experienced by children, women, persons with disabilities and older persons in The Gambia.

3.3. Holistic

The policy recognizes the inextricable link between online and offline risks and harms. Online and offline exploitation and abuse often share common root causes related to poverty, harmful social norms and gender inequality. The African Union acknowledges the evidence that shows "children who are vulnerable offline are also more likely to be vulnerable online, hence protective offline factors can also reduce exposure to online risks. Offline factors that create vulnerability or protection influence how children engage with the online environment."⁴¹ There is therefore a need to better understand the connections between children's online and offline experiences, and develop holistic solutions that tackle all forms of harm and violence together, which includes strengthening systems and services of prevention and response for all forms of violence, abuse and exploitation.

3.4. Inclusive

The policy takes into account the intersectionalities that are likely to exacerbate individuals' vulnerability. For example, children with disabilities or older women can experience increased vulnerability to online risks due to intersecting factors related to their specific circumstances. Children with disabilities may be more targeted by cyberbullying or online harassment because of their perceived differences or vulnerabilities, and they may have less access to resources that teach online safety, or their caregivers may lack knowledge about digital risks. Older women may be more targeted by online scams and fraud due to less familiarity with digital technologies and online safety practices, and they may have difficulty recognizing and reporting fraudulent activities. Addressing these vulnerabilities requires tailored approaches, including specialized awareness and education on online safety, as well as support systems and accessibility considerations to ensure all the different vulnerable groups can navigate the digital world safely.

⁴¹ African Union, "The African Union Child Online Safety and Empowerment Policy," February 2024, <https://au.int/en/documents/20240521/african-union-child-online-safety-and-empowerment-policy>.

3.5. Multi-sectoral

The policy recognizes that the responsibility for online protection and safety involves many people, specializations and organizations. Therefore, it is important to establish a multi-sector platform that enables engagement with relevant stakeholders. They include representatives from government institutions in the education, ICT, justice, health and social protection sectors, human rights organizations, civil society organizations representing children and vulnerable groups, academia and training institutions, and private sector players, including internet service providers, global system for mobile communication (GSM) operators and content developers, among others.

3.6. Regional and Global Collaboration

The policy is aware of the cross-border and transnational nature of online harm, exploitation and abuse. Therefore, regional and global collaboration is needed for conducting investigations, sharing information and resources, exchanging expertise and good practices, and harmonizing legislation and regulations for more effective online protection of children and vulnerable groups.

3.7. Participation of Children and Vulnerable Groups

The policy recognizes the need to ensure the inclusive and meaningful participation of children and vulnerable groups in policymaking, program implementation, training development, product and service design and review, and monitoring and evaluation processes. Organizations representing children and vulnerable groups can help to engage children and vulnerable groups in these processes, ensuring that their needs and concerns are effectively addressed.

4.0 Policy Objectives

The Gambia's National Child and Vulnerable Groups Online Protection Policy aims to provide a common vision and understanding of what children and vulnerable groups online protection entails. In line with the above-mentioned guiding principles, the policy promotes a unified approach for greater and accelerated impact toward ensuring that the rights of all children and vulnerable groups are respected, protected and fulfilled in the digital environment. The policy intends to strengthen coordination, cooperation and collaboration across sectors and borders to effectively prevent and respond to all forms of online risks and harms that children and vulnerable groups are exposed to in The Gambia.

5.0 Vision and Mission

The vision is to ensure a safe, secure and supportive digital environment for all children and vulnerable groups in The Gambia, where their rights are protected, their well-being is prioritized, and they are empowered to leverage the full potential of digital technology for sustainable growth and development.

The mission is to establish and implement a comprehensive online protection framework in The Gambia that upholds the rights and well-being of all children and vulnerable groups by leveraging global standards, best practices, global and regional partnerships, and collaboration between government, industry, civil society, educators and families.

6.0 Policy Pillars for Child and Vulnerable Groups Online Protection in The Gambia

Taking into consideration the wide spectrum of online risks and harms, the Gambian context and national commitments to global and regional frameworks, The Gambia's National Child and Vulnerable Groups Online Protection Policy establishes a set of policy actions across 11 policy pillars.

6.1 Enhance Governance

Policy Action 1.1: Establish a section under the National Cybersecurity Coordination Directorate to lead policy implementation, coordination, monitoring and evaluation

As indicated in the National Cybersecurity Strategy and Action Plan of The Gambia 2022–2026, a section under the National Cybersecurity Coordination Directorate will be established to handle matters relating to child online exploitation and abuse. This section will be extended to include other vulnerable groups and take the lead in steering and coordinating the implementation of the National Child and Vulnerable Groups Online Protection Policy. This section will also be responsible for ensuring sufficient resource allocation for policy implementation, as well as for monitoring progress and evaluating the impact of the National Child and Vulnerable Groups Online Protection Policy.

Policy Action 1.2: Establish a multi-sector stakeholder committee to engage relevant stakeholders

Since the online protection of children and vulnerable groups is a complex and multi-sector endeavor, a multi-sector stakeholder committee will be established to engage relevant stakeholders from government, the private sector, civil society, academia and training, social services, law enforcement and the judiciary, the technical community, and the international development and human rights community in providing expertise and supporting the implementation of the National Child and Vulnerable Groups Online Protection Policy.

Policy Action 1.3: Develop mechanisms to enable the participation of children and vulnerable groups in policymaking, implementation and review

Mechanisms will be developed to enable the participation of children and vulnerable groups in policymaking, implementation and review of the National Child and Vulnerable Groups Online Protection Policy. Existing structures and networks such as the Children National Assembly of The Gambia, women's networks, registered organizations representing persons with disabilities under The Gambia Federation of the Disabled, and associations of parents and caregivers, will be leveraged to engage children and vulnerable populations throughout the process of policy implementation, monitoring and evaluation.

6.2 Build Institutional Capacity

Policy Action 2.1: Assess the institutional capacity needs of the newly established section under the National Cybersecurity Coordination Directorate that will lead policy implementation, coordination, monitoring and evaluation

Building institutional capacity to lead the implementation, coordination, monitoring and evaluation of the national policy is essential to its success. Upon establishment of the section, a first step will be to conduct a comprehensive assessment of the institutional capacity gaps in skills, resources and infrastructure.

Policy Action 2.2: Strengthen institutional capacity based on the gap assessment

The institutional capacity of the newly-established section under the National Cybersecurity Coordination Directorate to lead policy implementation, coordination, monitoring and evaluation will be strengthened in multiple ways depending on needs. Actions will include the identification and mobilization of actors for the multi-sector stakeholder committee that can contribute expertise in all policy pillars of the National Child and Vulnerable Groups Online Protection Policy. In addition, training workshops, exchange programs and collaborations with national, regional and international institutions will be facilitated to address any skills gap and learn best practices. In order to enhance data collection, reporting and monitoring systems to track progress and improve policymaking, investment in digital platforms, dashboards and performance management systems will be considered.

6.3 Review and Reform Legal and Regulatory Frameworks

Policy Action 3.1: Review legal and regulatory frameworks

One of the objectives in the National Cybersecurity Strategy and Action Plan of The Gambia 2022–2026 is the enactment of legislation for child online protection in accordance with regional and global standards. This will involve undertaking a comprehensive legislative and regulatory review in the areas of ICT, cybersecurity, consumer protection, data protection, human trafficking, criminal justice, education, health, social welfare, and the rights of children, women, persons with disabilities and older persons, etc. The review will identify gaps in protecting children and vulnerable groups in the digital environment from all forms of online risks and harms, including content, contact, conduct and contract risks, as well as the risks and harms from the use of AI technologies.

In line with global and regional standards and best practices, the review will assess whether the legal and regulatory frameworks of The Gambia address: (1) the prohibition of all forms of violence, exploitation and abuse against children and vulnerable groups in the digital environment; (2) higher levels of protection for the collection and processing of children and vulnerable groups' data; (3) the obligations of digital service providers in ensuring the online safety of children and vulnerable groups; (4) the facilitation of investigation, prosecution and sentencing of online offences that violate children's and human rights; (5) preventive measures to protect children and vulnerable groups online; and (6) provision of effective response, recovery and rehabilitation that are in the best interest of children and vulnerable groups.

Policy Action 3.2: Strengthen legal and regulatory frameworks

Based on recommendations from the review process, actions will be taken to strengthen the legal and regulatory structures and enforcement mechanisms for the online protection of children and vulnerable groups in The Gambia, in line with global and regional standards and best practices.

6.4 Strengthen Response and Support Systems

Policy Action 4.1: Strengthen systems of law enforcement and the judiciary in addressing online risks and harms

Law enforcement and the judicial system will be strengthened to effectively prevent and respond to all forms of online risks and harms. This will include strengthening institutional systems with tools and guidelines to investigate and prosecute online offences in collaboration with regional and international organizations. Where possible, children who find themselves in conflict with the law, for example, in cases of cyberbullying or self-generated sexual content, will be diverted from

the criminal justice system, and opportunities for counselling or restorative justice will be preferred.

Policy Action 4.2: Strengthen social service and child protection systems in addressing online risks and harms

Social service and child protection systems will be strengthened to effectively prevent and respond to all forms of online risks and harms. This will involve ensuring that children and vulnerable groups, as well as their family and caregivers, have access to user-friendly reporting of online risks and harms, and quality support and recovery services, including mental health and psychosocial support, case management and referral pathways, across multiple channels such as helplines, schools and one-stop community centers. The systems will be strengthened through collaborations between government, civil society, the private sector and the international community in the development of protocols and guidance for the social service and child protection workforce.

Policy Action 4.3: Strengthen the national helpline and one-stop centers for incident reporting of online exploitation and abuse, and supporting survivors and at-risk groups

Protocols and guidelines will be established for receiving, prioritizing, actioning and referring reports on online exploitation and abuse received via the national helpline and one-stop centers. The national helpline and one-stop centers currently provide comprehensive services to survivors of gender-based and sexual violence and abuse, and will be extended to include services for online exploitation and abuse. Staff and volunteers of the national helpline and one-stop centers will be trained to implement these protocols and guidelines to better support children and vulnerable groups.

6.5 Engage Digital Service Providers

Digital service providers, including internet service providers, GSM operators and content developers, will be engaged to ensure the effective implementation of the National Child and Vulnerable Groups Online Protection Policy. This will include the development of effective measures to prevent, detect, take down and report online risks and harms affecting children and vulnerable groups.

6.5.1 Internet Service Providers

Policy Action 5.1: Develop codes of conduct, protocols and/or guidelines for internet service providers on the protection of children and vulnerable groups online

Government will work with internet service providers to establish codes of conduct, protocols and/or guidelines to protect children and vulnerable groups online. The codes of conduct, protocols and/or guidelines will include requirements for: (1) maintaining a secure network to protect all users, especially children and vulnerable groups, from online risks and harms; (2) reporting illegal and harmful content and activities online; (3) blocking access to illegal and harmful websites and content online, ensuring that the entire process is transparent, with review and appeals mechanisms in place for users; (4) educating users about online safety, targeting children and vulnerable groups, in collaboration with government and civil society; (5) developing interactive and engaging materials on online safety and effective tools to protect children and vulnerable groups (e.g., safe browsing modes, age-appropriate content filters, parental controls and usage limits or time restrictions on apps and internet access); and (6) ensuring the responsible and ethical use of AI for automated systems such as content filtering and blocking.

6.5.2 GSM Operators

Policy Action 5.2: Develop codes of conduct, protocols and/or guidelines for GSM operators on the protection of children and vulnerable groups online

Government will work with GSM operators to establish codes of conduct, protocols and/or guidelines to protect children and vulnerable groups online. The codes of conduct, protocols and/or guidelines will include requirements for: (1) maintaining a secure mobile network to protect all users, especially children and vulnerable groups, from online risks and harms; (2) reporting illegal and harmful content and activities online; (3) blocking access to illegal and harmful content and services, ensuring that the entire process is transparent, with review and appeals mechanisms in place for users; (4) educating users about online safety, targeting children and vulnerable groups, in collaboration with government and civil society; (5) developing interactive and engaging materials on online safety and effective tools to protect children and vulnerable groups (e.g., safe modes, age-appropriate content filters, parental controls and usage limits or time restrictions on apps and internet access); and (6) ensuring the responsible and ethical use of AI for automated systems such as content filtering and blocking.

6.5.3 Content Developers

Policy Action 5.3: Develop codes of conduct, protocols and/or guidelines for content developers on the protection of children and vulnerable groups online

Government will work with content developers, including app creators, website designers, game developers and social media platform operators, to establish codes of conduct, protocols and/or guidelines to protect children and vulnerable groups online. The codes of conduct, protocols and/or guidelines will include requirements for: (1) developing age-appropriate, gender-sensitive and disability-inclusive content, products and services; (2) developing and implementing safety-by-design and privacy-by-design features in their products and services, prioritizing the best interests of children and vulnerable groups; (3) implementing accessible and user-friendly mechanisms for users to report illegal and harmful content and activities; (4) reporting of illegal and harmful online content and activities to officials; (5) notice and takedown of illegal and harmful content online; (6) educating users about online safety, targeting children and vulnerable groups, in collaboration with government and civil society; (7) developing interactive and engaging materials on online safety and effective tools to protect children and vulnerable groups (e.g., tools to identify and verify the age of users, user-friendly privacy and security settings, the flagging of potentially harmful content, content labelling on the age-appropriateness or trustworthiness of content, parental controls); and (8) ensuring the responsible and ethical use of AI for automated systems such as automated content moderation, abuse detection and age verification.

6.6 Improve Training for Law Enforcement, Judiciary and Social Service

Policy Action 6.1: Enhance the capacity of law enforcement and the judiciary in addressing online risks and harms

In collaboration with institutions that are training law enforcement officers, lawyers, prosecutors and judges, a training module on online protection issues will be developed and incorporated in pre-service and in-service training courses for officials from law enforcement and the judiciary. The training module will aim to improve the understanding of the wide spectrum of online risks and harms and their impacts on children and vulnerable groups, the patterns of offending and profiles of offenders, effective methods and techniques for investigating, prosecuting and hearing

cases of online exploitation and abuse of children and vulnerable groups, and justice procedures that are child-friendly, age-appropriate, gender-sensitive and disability-inclusive.

Policy Action 6.2: Enhance the capacity of the social service and child protection workforce in addressing online risks and harms

In collaboration with institutions that are training the social service and child protection workforce in the mental health, psychology and social work fields, a training module on online protection issues will be developed and incorporated in pre-service and in-service training courses for professionals of the social service and child protection workforce. The training module will aim to support children and vulnerable groups in mitigating their exposure to online risks and harms. Upon completion of the training module, social service and child protection professionals will be able to recognize the signs and symptoms of online exploitation and abuse, and provide age-appropriate, gender-sensitive and disability-inclusive counselling, case management services and referrals to legal, medical, psychosocial, health and other services.

6.7 Incorporate Online Safety in Education

Policy Action 7.1: Integrate online safety education for children into school curricula, including as a critical component of digital literacy education

A standardized national online safety module will be developed and rolled-out for integration into digital literacy education in schools. The online safety module will cover all forms of online risks and harms, and will be age-appropriate, gender-sensitive and disability-inclusive. The content and design of the module will be shaped by international online safety education models, evidence-based research on the national and local contexts, and insights and experiences of children and vulnerable groups in The Gambia. Pre-service and in-service teachers will be trained to adapt the module to local contexts and effectively deliver the module.

Policy Action 7.2: Develop protections and procurement standards for education technology and technology used in schools

Protocols and guidelines will be developed for the procurement of education technology and technology used in schools, including requirements for companies designing and supplying the technology to: (1) incorporate safety-by-design and privacy-by-design principles; (2) conduct child rights impact assessments; (3) not collect and process data of children and vulnerable groups for the purposes of profiling, behavioral advertising and other uses unrelated to the purpose of providing education; and (4) report data security breaches and have effective remedies in place.

6.8 Raise Public Awareness on Online Safety

Policy Action 8.1: Organize targeted awareness raising campaigns on online safety for children and vulnerable groups, and their parents and caregivers

Targeted awareness raising campaigns on online safety for children, parents and caregivers, and vulnerable groups will be designed and carried out through collaborations between government, social protection programs, civil society, community groups, youth clubs, women's networks, religious institutions, academia, the private sector, media agencies, international development organizations, and children and vulnerable groups themselves. The messages and materials will help targeted groups better understand online risks, as well as take actions to mitigate harms, report illegal and harmful content and activities, and seek redress. The messages and materials will be disseminated across multiple channels and languages to maximize reach to targeted

groups. Special attention will be made to ensure that the messages and materials are accessible to persons with disabilities and older persons.

6.9 Promote Research and Development

Policy Action 9.1: Develop a plan for data collection, monitoring and evaluation to inform policy implementation and improvement

In line with the monitoring and evaluation framework outlined in Section 8, a plan will be developed for data collection, monitoring and evaluation to provide the data and evidence necessary for the implementation and updating of this policy. The plan will focus on engaging with relevant partners from academia, civil society, the private sector and international development organizations to undertake research to better understand children and vulnerable groups' online experience in The Gambia, the impact on their health and well-being, and how they cope with online risks and harms. Research will also focus on assessing the effectiveness and impact of children and vulnerable groups online protection programs and initiatives, and support the development of tools and services to ensure children and vulnerable groups' safety online. The data collected will be disaggregated by age, sex, disability and geographical location. Data collection and research relating to children and vulnerable groups will respect their privacy and meet the highest ethical standards.

6.10 Enhance International Cooperation

Policy Action 10.1: Formalize cooperations with international and regional organizations for joint investments in the online protection of children and vulnerable groups

Memorandums of understanding will be established with international and regional organizations to enhance the online protection of children and vulnerable groups, including in strengthening governance and institutional capacity, reviewing and reforming legal and regulatory frameworks, improving response and support systems, improving training, education and public awareness, and promoting research and development that contribute toward a safer digital environment for all.

Policy Action 10.2: Participate in the international and regional exchange of knowledge and experience on the online protection of children and vulnerable groups

Online protection stakeholders in The Gambia will promote and contribute to the international and regional sharing of expertise, good practices and lessons learned from developing and implementing the National Child and Vulnerable Groups Online Protection Policy. This will include the sharing of data, evidence, resources, protocols, guidelines, tools and techniques to enable a safer digital environment for all.

6.11 Integrate Child and Vulnerable Groups Online Protection in Emergencies and Pandemics

Policy Action 11.1: Develop crisis response protocols to ensure the continuity of online protection for children and vulnerable groups during emergencies and pandemics

A set of multi-sector crisis response protocols will be developed to strengthen the resilience of online protection systems for children and vulnerable groups. These crisis response protocols that outline the roles and responsibilities of key stakeholders, including law enforcement and the judiciary, the social service and child protection workforce, schools, and digital service providers, will be activated during emergencies, including pandemics, disasters or political instability. The

protocols will include measures to deal with rising incidences of online violence, cybercrimes, and disinformation and misinformation during crisis situations.

7.0 Institutional Framework for Implementation

The institutional framework for implementation sets out the lead agency and the stakeholders that will be engaged to coordinate actions toward achieving each policy action across the 11 policy pillars.

Policy Areas	Lead Agency	Stakeholders
Policy Pillar 1: Enhance Governance		
Policy Action 1.1: Establish a section under the National Cybersecurity Coordination Directorate to lead policy implementation, coordination, monitoring and evaluation	NCCD	GICTA, GM-CSIRT, MOCDE, PURA
Policy Action 1.2: Establish a multi-sector stakeholder committee to engage relevant stakeholders	NCCD	GICTA, GM-CSIRT, MOBSE, MOCDE, MOGCSW, MOH, MOHERST, MOI, MOJ, NAATIP, NHRC, ONS, PURA, GCSA, ITAG, ISPs, GSM operators, content developers, civil society, academia, international development organizations, UN agencies
Policy Action 1.3: Develop mechanisms to enable the participation of children and vulnerable groups in policymaking, implementation and review	NCCD	MOGCSW, Children National Assembly, Community Child Protection Committees, CEDAG, ChildFund The Gambia, CPA, ISRA, National Youth Council, SOS Children's Villages, NGBV, SHOAW Gambia, Gambia Federation of the Disabled, organizations representing persons with disabilities and older persons, associations of parents and caregivers, UN agencies
Policy Pillar 2: Build Institutional Capacity		
Policy Action 2.1: Assess the institutional capacity needs of the newly established section under the National Cybersecurity Coordination Directorate that will lead policy implementation, coordination, monitoring and evaluation	NCCD	GICTA, MOCDE, PURA
Policy Action 2.2: Strengthen institutional capacity based on the gap assessment	NCCD	GICTA, MOCDE, PURA
Policy Pillar 3: Review and Reform Legal and Regulatory Frameworks		
Policy Action 3.1: Review legal and regulatory frameworks	MOCDE	GICTA, GM-CSIRT, MOBSE, MOGCSW, MOH, MOI, MOJ, NAATIP, ONS, PURA, National Assembly's Select Committee on Health, Women, Children, Refugee, Disaster and Humanitarian Relief
Policy Action 3.2: Strengthen legal and regulatory frameworks	MOCDE	GICTA, GM-CSIRT, MOBSE, MOGCSW, MOH, MOI, MOJ, NAATIP, ONS, PURA, National Assembly's Select Committee on Health, Women, Children, Refugee, Disaster and Humanitarian Relief
Policy Pillar 4: Strengthen Response and Support Systems		
Policy Action 4.1: Strengthen systems of law enforcement and the judiciary in addressing online risks and harms	MOI / MOJ	Gambia Police Force, Gambia Police Female Network, Female Lawyers Association, Children's Court, Juvenile Wing of the Prison Service, GM-CSIRT, MOCDE, MOGCSW, ONS
Policy Action 4.2: Strengthen social service and child protection systems in addressing online risks and harms	MOGCSW	GM-CSIRT, MOCDE, MOH, Community Child Protection Committees, ChildFund The Gambia, CPA, SOS Children's Villages, NGBV, SHOAW

Policy Areas	Lead Agency	Stakeholders
		Gambia, Gambia Federation of the Disabled, UN agencies
Policy Action 4.3: Strengthen the national helpline and one-stop centers for incident reporting of online exploitation and abuse, and supporting survivors and at-risk groups	MOGCSW	GM-CSIRT, MOCDE, MOH, National helpline, one-stop centers
Policy Pillar 5: Engage Digital Service Providers		
Policy Action 5.1: Develop codes of conduct, protocols and/or guidelines for internet service providers on the protection of children and vulnerable groups online	MOCDE	GICTA, GM-CSIRT, PURA, MOGCSW, Africell, Comium, DK Telecom, Gamtel, INET, Netpage, Qcell, Unique Solutions, SIXP, organizations representing children and vulnerable groups
Policy Action 5.2: Develop codes of conduct, protocols and/or guidelines for GSM operators on the protection of children and vulnerable groups online	MOCDE	GICTA, GM-CSIRT, PURA, MOGCSW, Africell, Comium, Gamcel, Qcell, organizations representing children and vulnerable groups
Policy Action 5.3: Develop codes of conduct, protocols and/or guidelines for content developers on the protection of children and vulnerable groups online	MOCDE	GICTA, GM-CSIRT, PURA, MOGCSW, GamCON, GCSA, ITAG, app creators, website designers, game developers, social media platform operators, organizations representing children and vulnerable groups
Policy Pillar 6: Improve Training for Law Enforcement, Judiciary and Social Service		
Policy Action 6.1: Enhance the capacity of law enforcement and the judiciary in addressing online risks and harms	MOI / MOJ	Gambia Police Force, Gambia Police Female Network, Female Lawyers Association, Children's Court, Juvenile Wing of the Prison Service, MOCDE, MOGCSW, ONS
Policy Action 6.2: Enhance the capacity of the social service and child protection workforce in addressing online risks and harms	MOGCSW	MOCDE, MOH, Community Child Protection Committees, ChildFund The Gambia, CPA, SOS Children's Villages, NGBV, SHOAW Gambia, Gambia Federation of the Disabled, UN agencies
Policy Pillar 7: Incorporate Online Safety in Education		
Policy Action 7.1: Integrate online safety education for children into school curricula, including as a critical component of digital literacy education	MOBSE	MOCDE, MOGCSW, MOHERST
Policy Action 7.2: Develop protections and procurement standards for education technology and technology used in schools	MOBSE	MOCDE, MOGCSW, MOHERST, education technology companies
Policy Pillar 8: Raise Public Awareness on Online Safety		

Policy Areas	Lead Agency	Stakeholders
Policy Action 8.1: Organize targeted awareness raising campaigns on online safety for children and vulnerable groups, and their parents and caregivers	MOGCSW	MOBSE, MOCDE, MOH, Gambia Broadcasting Association, Gambia Press Union, Children National Assembly, CEDAG, ChildFund The Gambia, CPA, SOS Children's Villages, National Youth Council, NGBV, SHOAW Gambia, Gambia Federation of the Disabled, organizations representing persons with disabilities and older persons, associations of parents and caregivers, religious institutions, academia, the private sector, media agencies, international development organizations, UN agencies
Policy Pillar 9: Promote Research and Development		
Policy Action 9.1: Develop a plan for data collection, monitoring and evaluation to inform policy implementation and improvement	MOCDE	Bureau of Statistics, GICTA, MOBSE, MOGCSW, MOH, MOHERST, PURA
Policy Pillar 10: Enhance International Cooperation		
Policy Action 10.1: Formalize cooperations with regional and global organizations for joint investments in the online protection of children and vulnerable groups	MOCDE	GICTA, GM-CSIRT, MOBSE, MOGCSW, MOI, MOJ, African Union, African Development Bank, ECOWAS, EU, INTERPOL, ITU, UNICEF, UN Women and other UN agencies, World Bank
Policy Action 10.2: Participate in the international and regional exchange of knowledge and experience on the online protection of children and vulnerable groups	MOCDE	GICTA, GM-CSIRT, MOBSE, MOGCSW, MOI, MOJ, African Union, African Development Bank, ECOWAS, EU, INTERPOL, ITU, UNICEF, UN Women and other UN agencies, World Bank
Policy Pillar 11: Integrate Child and Vulnerable Groups Online Protection in Emergencies and Pandemics		
Policy Action 11.1: Develop crisis response protocols to ensure the continuity of online protection for children and vulnerable groups during emergencies and pandemics	MOCDE	GICTA, GM-CSIRT, MOBSE, MOGCSW, MOH, MOI, MOJ, NAATIP, NDMA, ONS, PURA, National Assembly's Select Committee on Health, Women, Children, Refugee, Disaster and Humanitarian Relief, Red Cross and Red Crescent Societies, humanitarian response agencies, civil society, media agencies, UN agencies

Notes: CEDAG = Child and Environment Development Association; CPA = Child Protection Alliance; ECOWAS = Economic Community of West African States; EU = European Union; GCSA = Gambia Cyber Security Alliance; GICTA = Gambia Information Communications Technology Agency; GM-CSIRT = The Gambia Computer Security Incident Response Team; GSM = Global System for Mobile Communication; INTERPOL = International Criminal Police Organization; ISP = Internet Service Provider; ISRA = Institute for Social Reformation and Action; ITAG = Information Technology Association of The Gambia; ITU = International Telecommunication Union; MOBSE = Ministry of Basic and Secondary Education; MOCDE = Ministry of Communications and Digital Economy; MOGCSW = Ministry of Gender, Children and Social Welfare; MOH = Ministry of Health; MOHERST = Ministry of Higher Education, Research, Science and Technology; MOI = Ministry of Interior; MOJ = Ministry of Justice; NAATIP = National Agency Against Trafficking in Person; NCCD = National Cybersecurity Coordination Directorate; NDMA = National Disaster Management Agency; NGBV = Network Against Gender Based Violence; NHRC = National Human Right Commission; ONS = Office of National Security; PURA = Public Utilities Regulatory Authority; SHOAW = Stop Harassment and Online Abuses of Women and Girls; SIXP = Serekunda Internet Exchange Point; UN = United Nations; UNICEF = United Nations Children's Fund.

8.0 Monitoring and Evaluation Framework

The newly-established section under the National Cybersecurity Coordination Directorate to lead and steer the implementation of the National Child and Vulnerable Groups Online Protection Policy will be responsible for tracking progress and monitoring and evaluating the outcomes of the policy. A progress report will be produced on an annual basis. The monitoring and evaluation framework below provides measurable key performance indicators and data collection methods for each policy action. Policy outcomes will be assessed against the United Nations standard evaluation criteria of effectiveness, efficiency, sustainability, relevance and impact. All data collected will be disaggregated by age, sex, disability and geographical location. The monitoring and evaluation process will also document good practices and lessons learned, and will include feedback from relevant stakeholders and citizens, which will be used for policy revision and improvements. Key findings of evaluations will be shared with relevant stakeholders and made publicly available.

Policy Area	Key Performance Indicator	Data Source / Data Collection Method
Policy Pillar 1: Enhance Governance		
Policy Action 1.1: Establish a section under the National Cybersecurity Coordination Directorate to lead policy implementation, coordination, monitoring and evaluation	Indicator 1.1.1: A section under the National Cybersecurity Coordination Directorate established to lead policy implementation, coordination, monitoring and evaluation	Official document approving or announcing launch of section, interviews with staff members
Policy Action 1.2: Establish a multi-sector stakeholder committee to engage relevant stakeholders	Indicator 1.2.1: A multi-sector stakeholder committee established Indicator 1.2.2: No. of committee meetings held	Official document approving or announcing establishment of committee, meeting minutes, interviews with committee members
Policy Action 1.3: Develop mechanisms to enable the participation of children and vulnerable groups in policymaking, implementation and review	Indicator 1.3.1: Mechanisms for the participation of children and vulnerable groups established Indicator 1.3.2: No. of consultations held with children and vulnerable groups	Official document approving or announcing mechanisms, consultation reports, feedback from children and vulnerable groups that participated in consultations
Policy Pillar 2: Build Institutional Capacity		
Policy Action 2.1: Assess the institutional capacity needs of the newly established section under the National Cybersecurity Coordination Directorate that will lead policy implementation, coordination, monitoring and evaluation	Indicator 2.1.1: Institutional capacity assessment of the section conducted	Report of the institutional capacity assessment of the section, interviews with assessors and staff members

Policy Area	Key Performance Indicator	Data Source / Data Collection Method
Policy Action 2.2: Strengthen institutional capacity based on the gap assessment	Indicator 2.2.1: No. of actions implemented to strengthen institutional capacity Indicator 2.2.2: No. of partnerships established between the section and other entities to implement the policy	Plan of action for institutional capacity building, progress reports, surveys or interviews with section staff and partners
Policy Pillar 3: Review and Reform Legal and Regulatory Frameworks		
Policy Action 3.1: Review legal and regulatory frameworks	Indicator 3.1.1: Review of legal and regulatory frameworks conducted	Report of the review of legal and regulatory frameworks
Policy Action 3.2: Strengthen legal and regulatory frameworks	Indicator 3.2.1: No. of legal and regulatory frameworks updated or developed to improve the online protection of children and vulnerable groups, in line with international children and human rights law	Official gazettes, decree documents, government notices or decisions published
Policy Pillar 4: Strengthen Response and Support Systems		
Policy Action 4.1: Strengthen systems of law enforcement and the judiciary in addressing online risks and harms	Indicator 4.1.1: No. of tools and guidelines developed to investigate and prosecute online offences Indicator 4.1.2: No. of partnerships established with regional and international organizations to investigate and prosecute online offences	Developed tools and guidelines, memorandums of understanding, surveys or interviews with officials of law enforcement and the judicial system
Policy Action 4.2: Strengthen social service and child protection systems in addressing online risks and harms	Indicator 4.2.1: No. of tools and guidelines developed to support social service and child protection systems in addressing online risks and harms Indicator 4.2.2: No. of children and vulnerable groups that experienced online risks and harms received support, case management and/or referrals to legal, medical, psychosocial, health and other services	Developed tools and guidelines, data collected from social service and child protection databases and information systems, surveys or interviews with the social service and child protection workforce
Policy Action 4.3: Strengthen the national helpline and one-stop centers for incident reporting of online exploitation and abuse, and supporting survivors and at-risk groups	Indicator 4.3.1: No. of tools and guidelines developed to support the national helpline and one-stop centers in addressing online risks and harms Indicator 4.3.2: No. and percentage of children and vulnerable groups contacting the national helpline and one-stop centers reported incidences of online exploitation and abuse Indicator 4.3.3: No. and percentage of children and vulnerable groups contacting the national helpline and one-stop centers and reported	Developed tools and guidelines, data collected from the national helpline and one-stop center databases and information systems, customer satisfaction surveys, interviews with staff and volunteers of the national helpline and one-stop centers

Policy Area	Key Performance Indicator	Data Source / Data Collection Method
	incidences of online exploitation and abuse satisfied with service experience and outcomes	
Policy Pillar 5: Engage Digital Service Providers		
Policy Action 5.1: Develop codes of conduct, protocols and/or guidelines for internet service providers on the protection of children and vulnerable groups online	Indicator 5.1.1: Codes of conduct, protocols and/or guidelines for internet service providers on the protection of children and vulnerable groups online developed and adopted Indicator 5.1.2: No. of reports received from internet service providers related to illegal and harmful content and activities online Indicator 5.1.3: No. of interventions initiated by internet service providers to ensure the online safety of children and vulnerable groups Indicator 5.1.4: No. of internet service providers with a corporate policy or plan for the online safety of children and vulnerable groups	Published codes of conduct, protocols and/or guidelines; letters and statements from internet service providers committing to the implementation of codes of conduct, protocols and/or guidelines; transparency reports
Policy Action 5.2: Develop codes of conduct, protocols and/or guidelines for GSM operators on the protection of children and vulnerable groups online	Indicator 5.2.1: Codes of conduct, protocols and/or guidelines for GSM operators on the protection of children and vulnerable groups online developed and adopted Indicator 5.2.2: No. of reports received from GSM operators related to illegal and harmful content and activities online Indicator 5.2.3: No. of interventions initiated by GSM operators to ensure the online safety of children and vulnerable groups Indicator 5.2.4: No. of GSM operators with a corporate policy or plan for the online safety of children and vulnerable groups	Published codes of conduct, protocols and/or guidelines; letters and statements from GSM operators committing to the implementation of codes of conduct, protocols and/or guidelines; transparency reports
Policy Action 5.3: Develop codes of conduct, protocols and/or guidelines for content developers on the protection of children and vulnerable groups online	Indicator 5.3.1: Codes of conduct, protocols and/or guidelines for content developers on the protection of children and vulnerable groups online developed and adopted Indicator 5.3.2: No. of reports received from content developers related to illegal and harmful content and activities online Indicator 5.3.3: No. of interventions initiated by content developers to ensure the online safety of children and vulnerable groups	Published codes of conduct, protocols and/or guidelines; letters and statements from content developers committing to the implementation of codes of conduct, protocols and/or guidelines; transparency reports

Policy Area	Key Performance Indicator	Data Source / Data Collection Method
	Indicator 5.3.4: No. of content developers with a corporate policy or plan for the online safety of children and vulnerable groups	
Policy Pillar 6: Improve Training for Law Enforcement, Judiciary and Social Service		
Policy Action 6.1: Enhance the capacity of law enforcement and the judiciary in addressing online risks and harms	Indicator 6.1.1: Training module on the online protection of children and vulnerable groups developed Indicator 6.1.2: Training plan for piloting and nationwide rollout of module developed Indicator 6.1.3: No. and percentage of officials from law enforcement and the judiciary trained to handle online safety cases affecting children and vulnerable groups Indicator 6.1.4: No. and percentage of trained officials who feel confident in recognizing and responding to incidences of online exploitation and abuse	Developed module and training plan, training registration and evaluation data, surveys or interviews with trained officials
Policy Action 6.2: Enhance the capacity of the social service and child protection workforce in addressing online risks and harms	Indicator 6.2.1: Training module on the online protection of children and vulnerable groups developed Indicator 6.2.2: Training plan for piloting and nationwide rollout of module developed Indicator 6.2.3: No. and percentage of officials from social service and child protection workforce trained to address online risks and harms Indicator 6.2.4: No. and percentage of trained officials who feel confident in recognizing and responding to incidences of online exploitation and abuse	Developed module and training plan, training registration and evaluation data, surveys or interviews with trained officials
Policy Pillar 7: Incorporate Online Safety in Education		
Policy Action 7.1: Integrate online safety education for children into school curricula, including as a critical component of digital literacy education	Indicator 7.1.1: Online safety module for schools developed and integrated into national digital literacy curricula Indicator 7.1.2: Plan for piloting and nationwide rollout of module developed Indicator 7.1.3: No. and percentage of teachers trained to deliver the module Indicator 7.1.4: No. and percentage of students completed the module Indicator 7.1.5: No. and percentage of students who completed the module are confident in navigating the digital environment safely and know how to report illegal and harmful online content and activities	Developed module and training plan, training registration and evaluation data from teachers, surveys or interviews with trainers and teachers, end-of-module assessment for students, surveys or interviews with students

Policy Area	Key Performance Indicator	Data Source / Data Collection Method
Policy Action 7.2: Develop protections and procurement standards for education technology and technology used in schools	Indicator 7.2.1: Protocols and guidelines for the procurement of education technology and technology used in schools developed and adopted	Developed protocols and guidelines, and schools' procurement guidelines, requests for proposals and contracts
Policy Pillar 8: Raise Public Awareness on Online Safety		
Policy Action 8.1: Organize targeted awareness raising campaigns on online safety for children and vulnerable groups, and their parents and caregivers	Indicator 8.1.1: National online safety awareness raising plan developed in collaboration with multi-sector stakeholders Indicator 8.1.2: No. of awareness raising campaigns organized Indicator 8.1.3: No. of children, women, persons with disabilities, older persons, parents and caregivers reached through the awareness raising campaigns Indicator 8.1.4: No. and percentage of children and vulnerable groups who know how to report illegal and harmful online content and activities, and seek help. Indicator 8.1.5: No. and percentage of parents and caregivers who believe they are able to help their children navigate the digital environment safely, speak to their children about online safety, and report illegal and harmful online content and activities	Developed plan, data collected from the awareness raising campaigns, questionnaire surveys for targeted groups reached by awareness raising campaigns, interviews with organizers of awareness raising campaigns
Policy Pillar 9: Promote Research and Development		
Policy Action 9.1: Develop a plan for data collection, monitoring and evaluation to inform policy implementation and improvement	Indicator 9.1.1: A plan for data collection, monitoring and evaluation to inform policy implementation and improvement developed Indicator 9.1.2: No. of research studies on the online safety of children and vulnerable groups conducted	Developed plan, monitoring and evaluation reports, research reports, interviews with relevant stakeholders
Policy Pillar 10: Enhance International Cooperation		
Policy Action 10.1: Formalize cooperations with regional and global organizations for joint investments in the online protection of children and vulnerable groups	Indicator 10.1.1: No. of memorandums of understanding related to the online protection of children and vulnerable groups established with international and regional organizations	Memorandums of understanding, interviews with relevant officials
Policy Action 10.2: Participate in the international and regional exchange of knowledge and experience on the online protection of children and vulnerable groups	Indicator 10.2.1: No. of international and regional events related to the online protection of children and vulnerable groups participated	Event outcome reports, interviews with relevant officials
Policy Pillar 11: Integrate Child and Vulnerable Groups Online Protection in Emergencies and Pandemics		

Policy Area	Key Performance Indicator	Data Source / Data Collection Method
Policy Action 11.1: Develop crisis response protocols to ensure the continuity of online protection for children and vulnerable groups during emergencies and pandemics	Indicator 11.1.1: Crisis response protocols for the online protection of children and vulnerable groups during emergencies and pandemics developed	Developed plan, situational analysis of crisis situations, interviews with relevant officials