REPUBLIC OF ZAMBIA

REPORT

OF THE

COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES ON CHILD ONLINE PROTECTION MEASURES IN ZAMBIA

FOR THE

FIFTH SESSION OF THE THIRTEENTH NATIONAL ASSEMBLY

Published by the National Assembly of Zambia

FOREWORD

Honourable Madam Speaker, the Committee on Media, Information and Communication Technologies has the honour to present its Report for the Fifth Session of the Thirteenth National Assembly on Child Online Protection Measures in Zambia. The Committee's functions are set out in Standing Order 205 (b) and 206 of the National Assembly of Zambia Standing Orders, 2024.

The Committee held ten meetings to consider the topical issue. In order to fully interrogate the issue, the Committee requested detailed memoranda from various stakeholders, who were later invited to speak to their written submissions and make clarifications on issues arising therefrom. The list of stakeholders is at Appendix II.

The Committee's Report is organised in two parts: Part I presents the findings from the Committee's deliberations on the topical issue, while Part II outlines the Committee's consideration of the Action-Taken Report on its Report for the Fourth Session of the Thirteenth National Assembly.

The Committee is grateful to all stakeholders who tendered both written and oral submissions. The Committee further wishes to thank you, Madam Speaker, for affording it an opportunity to carry out its work and also appreciates the services rendered by the Office of the Clerk of the National Assembly throughout its deliberations.

Eng Raphael S Mabenga, MP
CHAIRPERSON

April, 2026
LUSAKA

TABLE OF CONTENTS

ACRONYMS

AI –	Artificial Intelligence
COP –	Child Online Protection
ICT –	Information Communication Technologies
ISPs –	Internet Service Providers
ZICTA –	Zambia Information and Communications Technology Authority

1.0 Membership of the Committee

The Committee consisted of Eng Raphael S Mabenga, MP (Chairperson); Ms Melesiana Phiri, MP (Vice-Chairperson); Mr Sydney Mushanga, MP; Mr Andrew Z Lubusha, MP; Mr Romeo Kangombe, MP; Mr Andrew Tayengwa, MP; Mr Walusa Mulaliki, MP; Mr Chanda A B Katotobwe, MP; Mr Elias Daka, MP; and Mr Stanley Kakubo, MP.

PART I

2.0 Consideration of the Topical Issue

2.1 Child Online Protection Measures in Zambia

2.1.1 Background

Over the past decade, Zambia has experienced an unprecedented wave of digital transformation. Expanded access to Information and Communication Technologies (ICTs) coupled with a youthful and increasingly connected population has reshaped the nation's social and economic landscape. By June 2025, the Zambia Information and Communications Technology Authority (ZICTA) reported more than 24.5 million mobile subscriptions and over 13 million internet subscriptions, translating into a mobile penetration of 119 connections per 100 inhabitants and an internet penetration of sixty-four connections per 100 inhabitants.

For children, the internet has become a central part of daily life. It offers unparalleled opportunities to learn, communicate, socialise, and play, while also exposing them to diverse cultural and social ideas. The 2022 National Information Communication Technology (ICT) Survey revealed that 71 per cent of children with internet access used it primarily for social networking, followed by watching movies at 58.1 per cent, studying at 50 per cent, researching at 49.3 per cent, and downloading materials at 44 per cent. These findings highlight the growing role of the internet in children's education, learning, creativity, and social interaction. However, these same technologies that empower children also expose them to online harm that threaten their safety, privacy, mental health, and overall well-being. Online scams, cyber bullying, grooming, trafficking, and exposure to harmful or manipulative content are now common realities. It is against this backdrop that the Committee resolved to undertake a review of Child Online Protection (COP) Measures in Zambia.

2.1.2 Objectives of the Study

The objectives of the study were to:

(a) ascertain the adequacy of the legal, policy and institutional frameworks;
(b) appreciate the risks and threats faced by Zambian children online;
(c) learn the mechanisms in place for reporting online child abuse, exploitation,
(d) appreciate the role of state and non-state actors in promoting child online safety;
(e) understand the challenges, if any, in the implementation of COP measures; and

(f) make recommendations on how to strengthen the protection of Zambian children in the online environment.

2.2 Summary of Stakeholders' Submissions

A summary of the submissions from various stakeholders on the topical issue is presented below.

2.2.1 Adequacy of the Legal, Policy and Institutional Frameworks Governing Child Online Protection in Zambia

I. Legal Framework

The Committee was informed that Zambia's legal framework for COP was derived from a combination of child-specific legislation, cyber-related statutes, and international instruments. Further, the Constitution of Zambia guaranteed the protection of children against abuse, neglect, and exploitation, forming the foundational basis for child rights protection.

The Committee was informed that Zambia's COP measures were grounded in several key laws, as highlighted below:

(a) The *Cyber Crimes Act No. 4 of 2025*, criminalised Child Sexual Abuse Material (CSAM), online grooming, harmful content, electronic harassment and other online exploitation. It also established ZICTA's cyber-protection role, digital evidence frameworks and takedown procedures.

(b) The *Information and Communication Technologies Act, No. 15 of 2009*, empowered ZICTA to regulate Internet Service Providers (ISPs) and digital communications systems, including the removal or blocking of harmful online content.

(c) The *Children's Code Act, No. 12 of 2022*, governed all aspects of child protection, mandated reporting, criminalised sexual exploitation and established child safeguarding responsibilities. It applied to both online and offline abuse and made teachers and caregivers mandatory reporters.

(d) The Penal Code criminalised defilement, trafficking, prostitution of minors and related forms of exploitation.

(e) The *Anti-Gender-Based Violence Act, No. 1 of 2011,* provided protection for child victims of physical, emotional and sexual violence, including digitally facilitated abuse.

(f) The *Anti-Human Trafficking Act, No. 11 of 2008* covered trafficking and online recruitment or exploitation of children, including cross-border cases.

(g) The *Education Act, No. 23 of 2011* mandated schools to report child abuse and manage cases of cyber bullying or digital abuse within school settings.

II. Policy Frameworks

Stakeholders submitted that there were several policies around COP in Zambia as highlighted below.

(a) The National ICT Policy (2023) established the framework for digital transformation, focusing on accessibility, innovation, digital skills, e-services, and risk management. It emphasised the need to expand ICT infrastructure, promote digital literacy, and ensure safe and equitable access to technology.

(b) The Digital Transformation Strategy (2023-2027) operationalised the National ICT Policy by setting out concrete measures to embed digital technologies across all sectors of the economy and society. It prioritised connectivity, innovation, and digital inclusion, while promoting secure and resilient systems.

(c) The National Child Online Protection Strategy (2025-2029) was built on the Child Policy 2015-2012, ICT Policy 2023, and Digital Transformation Strategy 2023-2027 by translating broad objectives into targeted online safety interventions. It addressed risks such as cyber bullying, grooming, harmful content exposure and exploitation, while promoting awareness and resilience among children.

III. International Instruments

The Committee was informed that Zambia was a party to several international and regional instruments that provided a framework for COP and placed obligations on the State to safeguard children from both online and offline harm. These included the following:

(a) the United Nations Convention on the Rights of the Child (UNCRC) established the foundational principles for child protection, including the best interests of the child, protection from exploitation, and the right to safe access to information;

(b) the African Charter on the Rights and Welfare of the Child (ACRWC) reinforced child protection obligations within the African context by emphasising protection from abuse, exploitation, and harmful practices; and

(c) the International Telecommunication Union (ITU) COP Guidelines provided practical international standards for governments, regulators, industry, and civil society to create safer online environments for children.

2.2.2 Risks and Threats Faced by Zambian Children Online

The Committee was informed that the online environment presented significant risks and threats to children in Zambia, as reflected in the statistical evidence contained in the table below.

Table 1: Risks and Threats Faced by Zambian Children Online

Online Risks	**Awareness (%)**	**Exposure (%)**	**Victim (%)**
Phishing	18.4	6.4	0.8
Grooming	21.6	7.2	0.8
Terrorism	21.6	8.8	0.8
Online Defamation	29.6	11.2	0.8
Impersonation	31.2	11.2	0.8
Damage to Reputation	38.4	20	1.6
Identity Theft	41.6	22.3	3.2
Unwanted Sexting	44	26.4	8.8
Violence	44.8	26.4	1.6
Hate Speech	46.4	28.8	0.8
False Alarm	47.2	28.8	4
Financial Fraud	48.8	24.8	2.4
Fake Online Promotion	48.8	32.8	5.6
Hacking	61.6	31.2	7.2
Child Sexual Abuse Materials	62.4	33.6	4
Scams	72.8	49.6	4.8
Adult Pornography	79.2	49.6	8.8
Fake news	82.4	67.2	14.4
Cyber bullying	85.6	51.2	8

Source: 2022 National ICT Survey

The survey highlighted that awareness of online risks among children was relatively high at 51.2 per cent for cyber bullying and 67.2 per cent for fake news, while exposure and victimisation rates remained significant. Fake news and adult pornography showed the highest exposure levels, while unwanted sexting, cyberbullying, and fake news recorded the highest victimisation rates.

Stakeholders further submitted that several studies had been conducted on the risks faced by children in the online environment, which added an additional dimension to the country's understanding of the scope, nature, and prevalence of online threats affecting children. The Committee was informed that a key case by Burton and Bwalya (2022), under the United Nations Children Fund (UNICEF) Zambia, revealed that 9 per cent of children had actively looked for websites with information on how to take their own life. Almost one in ten or 10 per cent of children aged 9 to 12 years had actively sought out information on how to harm themselves, compared to 6 per cent of children aged 13 to 15, and 11 per cent of children aged 16 to 17. Similarly, one in ten or 10 per cent of children aged 9 to 12 had actively sought out information online on taking drugs, and 8 per cent had sought out websites on ways to be thin.

The Committee was further informed that a Zambia-based non-governmental coalition, Joining Forces Alliance (2023), published a policy brief indicating that more than 700 cases of online child abuse were reported in December 2021, including incidents of cyberbullying, harassment, and exposure to pornographic material. Furthermore, a Zambia Kids Online study conducted by Save the Children in Zambia revealed that

children were exposed to harmful information, harassment, and violence online. The report showed that 23.2 per cent of girls and 10.9 per cent of boys had been asked for sexual information about themselves online, further highlighting the imminent risks faced by Zambian children in the online environment.

2.2.3 Mechanisms in Place for Reporting Online Child Abuse, Exploitation, and Harmful Content

The Committee was informed that there were several mechanisms in place for reporting online child abuse, exploitation and harmful content, as highlighted below.

I. National Child Help Lines

The national telephone-based child protection help lines provided free and confidential support as follows:

(a) 116 Childline offered 24/7 counselling, psychosocial support, and referrals for children facing abuse, exploitation, mental health challenges, including other child-related risks, and was accessible across all mobile networks in multiple local languages; and

(b) 933 Lifeline supported adults reporting concerns about a child's welfare;

II. Online reporting Mechanisms

The digital reporting ecosystem included dedicated tools for identifying and removing CSAM as follows:

(a) the Internet Watch Foundation (IWF) and ZICTA CSAM Reporting Portal to anonymously report illegal CSAM Uniform Resource Locator (URLs), which were reviewed by trained analysts and removed through collaboration with international partners, including the IWF, ZICTA and Childline;

(b) the Young Cyber Online Protection Ambassadors (YOCUPA) – International Association of Internet Hotlines Member Hotline (INHOPE), launched in 2025, served as a national hotline for reporting online child sexual exploitation, enabling anonymous reporting, CSAM assessment and removal, and coordination with police and the International Criminal Police Organisation (INTERPOL);

(c) Zambia's INHOPE accreditation made it the third African country to operate an internationally recognised hotline for online child protection; and

(d) major social media platforms (Facebook, Instagram, TikTok and WhatsApp) provided in-app reporting tools for grooming, exploitation and cyberbullying, with national bodies such as Childline, police and YOCUPA handling follow-up and enforcement.

III. Law Enforcement Mechanisms

The Committee was informed that Zambia's law enforcement response to child protection relied on multiple mechanisms, including the 991 Emergency Line for immediate threats, specialised police units such as the Victim Support Unit (VSU) and Child Protection Unit for investigation and victim-centred responses, and the Cyber Crimes Unit for digital offences involving children. These mechanisms were supported by both traditional and digital reporting channels and coordinated with national and international partners.

IV. Community-Level Reporting Mechanisms

The Committee was informed that community-based structures, schools, one-stop centres and civil society organisations formed the first line of detection and response to child abuse and online harms. In addition, early identification, integrated victim services, and awareness initiatives complemented formal law enforcement and national coordination frameworks through local reporting.

Further, the local reporting mechanisms had achieved some success, with Childline/Lifeline Zambia maintaining a database of reported online abuse and exploitation cases, although the system remained inadequate. Furthermore, the ChildLine/Lifeline Zambia 2025 Report revealed that between January and October 2025, Childline/Lifeline Zambia recorded a total of 4,766 cases of online abuse and exploitation involving both boys and girls, compared to 7,572 cases recorded for the entire year of 2025. The most frequently reported incidents related to online addiction, cyber bullying, online harassment, and unwanted sexting as highlighted in the table below.

Table 1: Distribution of Reported Online Abuse Cases by Sex (Jan–Oct 2025)

Category	Boys	Girls	Total
Online Addiction	601	709	1,310
Cyberbullying	587	506	1,093
Exposure to Porn	0	5	5
Sextortion	0	3	3
Harassment	392	841	1,233
Unwanted Sexting	417	705	1,122
Total	**1,997**	**2,769**	**4,766**

Source: ChildLine/Lifeline Zambia 2025 Report

2.2.4 Role of State and Non-State Actors in Promoting Child Online Safety

The Committee was informed that effective COP in Zambia required collaborative engagement between state and non-state actors, given that children accessed digital platforms both within and beyond school environments. To that effect, State and non-state actors jointly formed a multi-layered protection ecosystem for children online and promoted child online safety.

I. Role of State Actors

The Committee was informed that State institutions played a central role in COP as highlighted below.

(i) **Policy and Regulatory Oversight**

The State was responsible for developing child-centred online safety policies integrated across early childhood, primary, secondary, and tertiary education frameworks. They were also responsible for ensuring that ICT integration aligned with child protection standards through curricula and school management policies, while strengthening the enforcement of existing laws.

(ii) **Capacity-Building and Supervision**

The State undertook training for teachers, caregivers, social workers, and law enforcement personnel on COP and safe ICT use. It also included the integration of online safety modules into teacher professional development programmes through the Teacher Education and Specialised Services (TESS) Directorate.

(iii) **Awareness and Public Engagement**

The State coordinated national campaigns targeting parents, guardians, and communities on cyber risks and reporting mechanisms, and promoted safe digital learning platforms such as the Learning Passport Zambia, managed by the Directorate of Open and Distance Education.

(iv) **Institutional Coordination**

The Ministry of Technology and Science led the National Child Online Protection Strategy (2025–2029), while ZICTA regulated the ICT sector, provided content filtering, hosted reporting platforms, and delivered public training. The Ministry of Community Development and Social Services managed welfare services and referral mechanisms, while the Ministry of Education, through TESS and the Curriculum Development Centre, oversaw guidance services, teacher training, and curriculum integration of online safety.

II. Role of Non-State Actors

The Committee was informed that non-state actors complemented Government efforts through advocacy, technical assistance, service delivery, and community engagement. Civil society organisations and Non-governmental organisations (NGOs) such as UNICEF, World Vision, Save the Children, ChildFund, and Lifeline/Childline Zambia supported policy implementation, awareness campaigns, research, and psychosocial services. They collaborated with schools to implement the Safe School Guidelines and online protection protocols.

More specifically, stakeholders submitted on the role of non-state actors in the promotion of child online safety, as outlined below.

(i) **Raising Awareness**

Non-state actors played a critical role in disseminating information on online protection. Given that the Government coverage in the dissemination of information about online safety was not guaranteed to reach far-flung areas, non-state actors had the capacity to support the Government by reaching a broader audience.

(ii) **Provide Support Services**

Non-state actors included a variety of institutions that offered a broad range of services, from counselling to paralegal services. The support services included, but were not limited to, reporting cases, providing vast information about online safety and offering training to parents and strategic stakeholders such as lawmakers in Parliament, teachers in schools, pastors in churches and lecturers in universities.

(iii) **Lobbying for Policy Changes and Formulation**

Non-state actors that were specialised in promoting the welfare of online safety had trained personnel and first-hand experience in working with victims and offenders of cybercrimes. They had the technical knowledge and could lobby for better and enhanced policies that were culturally specific to Zambia.

(iv) **Build the Capacity of Stakeholders**

Non-state actors leveraged their technical expertise to strengthen the capacity of key stakeholders, including law enforcement agencies, regulators, educators, civil society organisations, and the judiciary, through specialised training and skills development aimed at enhancing child online protection responses.

(v) **Research**

Non-state actors undertook rigorous research and produced actionable points of implementation for the legislatures and the Executive to implement.

2.2.5 Challenges in the Implementation of Child Online Protection Measures

The Committee learnt that despite the existence of legal, policy, institutional, and technological frameworks for child online protection, effective implementation in Zambia was still constrained. These challenges were particularly pronounced for young learners aged 3–5 years and other vulnerable groups. The constraints were interconnected and spanned technological, institutional, operational, socio-cultural, data, and resource dimensions, collectively limiting the reach, consistency, and effectiveness of COP measures as highlighted below.

I. Technological and Infrastructure Challenges

(i) Uneven Access to ICT Tools and Protective Technologies

The effectiveness of COP initiatives was undermined by uneven access to ICT infrastructure and limited awareness of protective technologies. Many schools, teachers, parents, and caregivers lacked appropriate digital devices, affordable software, and knowledge of built-in online safety features. At the same time, learners increasingly accessed the internet through personal devices outside school environments, where supervision and protective controls were minimal, increasing exposure to online risks.

(ii) Limited Technical Capacity in Schools

Most schools did not have dedicated ICT personnel to manage, monitor, and maintain online safety systems. Inadequate or poorly equipped

computer laboratories reduced the ability to supervise learners, apply content filters, and ensure safe digital engagement, particularly in rural and peri-urban areas.

(iii) Fragmented Integration of Digital Systems

Existing technological safeguards were not systematically linked to school-based reporting, referral and response mechanisms, reducing both preventive and remedial effectiveness. In addition, key Ministry and institutional digital platforms operated in silos, limiting centralised access to COP resources, guidance, and reporting tools.

(iv) Rapid Technological Change

Emerging risks, including Artificial Intelligence-generated deep fakes, online grooming, and increasingly sophisticated child sexual exploitation material, continued to outpace policy adaptation, institutional readiness, and technical response capacity.

II. Institutional and Operational Challenges

(i) Human Resource and Capacity Gaps

There were critical shortages of trained guidance counsellors, resulting in teachers providing counselling services alongside full teaching workloads. Limited training in digital safety and COP, particularly among early childhood educators, further weakened prevention, supervision, and response mechanisms for younger learners. In addition, many schools lacked standardised teaching materials and structured programmes for delivering age-appropriate digital literacy.

(ii) Weak Coordination and Enforcement

Inter-institutional coordination among the Ministry of Education, the Ministry of Technology and Science, ZICTA, the Ministry of Community Development and Social Services, and law enforcement agencies remained weak, leading to delays in reporting, referral, and case management. Enforcement of existing legislation and policies, including the *Cyber Security Act* and child protection frameworks, remained inconsistent at school, district, and community levels.

(iii) Infrastructure Limitations at School Level

Many schools lacked private, safe, and child-friendly spaces for counselling and reporting, which reduced learner confidence and willingness to disclose online abuse. Limited resources for documentation, follow-up, and referral further weakened institutional response systems.

III. Education, Awareness, and Socio-Cultural Challenges

(i) Low Levels of Digital Literacy and Awareness

Awareness of online risks and reporting mechanisms remained low among learners, parents, caregivers, and some educators, despite ongoing initiatives. Parental and caregiver involvement in online supervision and safety remained limited, particularly for younger children.

(ii) Stigma, Fear, and Misconceptions

Cultural perceptions that associated counselling with weakness discouraged help-seeking behaviour. Fear of retaliation, victim-blaming, and social stigma continued to inhibit reporting of online abuse cases.

(iii) Age-Specific Vulnerabilities

Children aged 3–17 remained highly dependent on adults for supervision and protection. Gaps in caregiver engagement and digital literacy disproportionately affected younger learners and children with disabilities.

(iv) Data, Reporting, and Response Gaps

Weak data systems and fragmented reporting mechanisms significantly limited evidence-based planning and accountability. Although reporting channels such as Childline 116, the GBV hotline (944), and online portals existed, reporting of online abuse remained low due to limited awareness and weak coordination among service providers. Further, there was no consolidated national data system on online child abuse. Available data was rarely age or sex disaggregated, and information sharing among institutions remained limited.

IV. Resource and Budgetary Constraints

The Committee was informed that resource limitations cut across all challenge areas and significantly constrained implementation. Limited financial allocations restricted the rollout of technological safeguards, capacity-building programmes, victim support services, and nationwide awareness campaigns. While the National Child Online Protection Strategy (2025–2029) provided a comprehensive framework, its estimated budget of approximately US$1.8 million remained insufficient to ensure nationwide coverage, particularly for rural, hard-to-reach schools and early childhood education settings.

2.3 Committee's Observations and Recommendations

Having engaged with stakeholders and examined their perspectives on Child Online Protection Measures in Zambia, the Committee presents its observations and recommendations as set out below.

2.3.1 Reporting Mechanism Awareness

The Committee observes that despite the existence of reporting channels, the reporting of incidents of child online abuse remains low, largely due to limited public awareness, inadequate digital literacy among children, parents, and caregivers, and weak coordination among responsible institutions. The Committee further notes with concern that key toll-free services, including the Childline/Lifeline Helpline (116) and the GBV Hotline (944), are often non-functional, which undermines timely reporting and response. In this regard, the Committee recommends the implementation of sustained, nationwide public awareness campaigns to actively publicise existing child online abuse reporting mechanisms. The Committee further recommends that the Government should ensure the consistent functioning, resourcing, and monitoring of toll-free help lines to guarantee reliable access to reporting and response services.

2.3.2 National Digital Safety Curriculum

The Committee observes that digital access among learners is increasing rapidly yet digital safety education remains inconsistently delivered and is not a core learning outcome. As a result, many learners lack age-appropriate knowledge and skills to identify online risks, practise responsible digital behaviour, and seek help when exposed to harm.

In this regard, the Committee recommends that the Ministry of Education should enforce mandatory integration of digital literacy and online safety education into the national school curriculum from primary through secondary levels, complemented by sustained awareness programmes for parents, teachers, and caregivers to strengthen understanding of online risks and appropriate protection measures.

2.3.3 Minimum Internet Safety Standards for Schools

The Committee observes with concern that although many schools provide learners with access to computers and internet services, the absence of standardised firewalls, content filtering, and safe search systems has resulted in inconsistent protection across school ICT environments. This gap exposes learners to harmful online content and limits the capacity of schools to monitor usage, enforce acceptable use policies, and respond effectively to online safety incidents.

The Committee, therefore, recommends that the Ministry of Education, in collaboration with ZICTA and other relevant authorities, devise and enforce mandatory minimum internet safety standards in all schools that provide learners with access to computers or the internet, including the deployment of firewalls, content filtering, safe search controls, and monitored internet activity for safeguarding and accountability purposes.

2.3.4 Limited Digital Literacy

The Committee observes that inadequate digital literacy among parents and guardians presents a major challenge, as they lack the technical knowledge required to install, configure, and manage parental control tools effectively. This often renders tools ineffective or allows children to bypass controls.

In this regard, the Committee recommends that the Government implement targeted digital literacy and parental empowerment programmes, in various languages, to equip parents and guardians with practical skills to install, configure, and manage parental control tools effectively. These programmes should be delivered through schools, community structures, and public awareness platforms to ensure that parental controls are properly utilised and not easily bypassed by children.

2.3.5 Internet Service Provider Safety Features

The Committee observes that most households lack network-level tools to filter harmful online content, leaving children exposed outside supervised environments such as schools.

In this regard, the Committee recommends that ZICTA develop and enforce regulations requiring ISPs to implement network-level family-safe filtering systems, supported by

transparent opt-in and opt-out controls, clearly defined content categories, and compliance monitoring measures that safeguard user privacy.

2.3.6 National Child Online Protection Coordination Team

The Committee observes that COP efforts in Zambia are fragmented across multiple institutions, policies, and initiatives, resulting in uneven implementation, limited coordination, and weak monitoring of risks and responses at the national level.

In this regard, the Committee recommends that the Government should strengthen and fully operationalise the existing National Child Online Protection framework by establishing a coordinated national mechanism through a National Child Online Protection coordination team to address fragmentation across stakeholders, institutions and initiatives. This team should focus on the creation of standardised child safety reporting and crisis escalation procedures, issuance of clear and harmonised guidelines for school digital policies and improved monitoring through publicly accessible data on key child online safety indicators.

2.3.7 Human Resource and Capacity Gaps

The Committee observes that human resource and capacity gaps continue to weaken Child Online Protection (COP) efforts in schools, including shortages of trained guidance counsellors, limited digital safety training for educators, and the absence of standardised materials for delivering age-appropriate digital literacy.

In this regard, the Committee recommends that the Ministry of Education introduce a mandatory national teacher training programme on child online protection and digital safety to strengthen prevention, supervision, and response capacity within schools.

2.3.8 Fragmented Integration of Digital Systems

The Committee observes that the integration of digital systems supporting COP remains disjointed, with technological safeguards not systematically linked to school-based reporting and response mechanisms, while institutional platforms continue to operate in silos, limiting coordinated access to resources and reporting tools.

In this regard, the Committee recommends that the Government should establish a centralised national database to systematically capture, track, and report online child exploitation cases, disaggregated by age, sex, and type of abuse, with inputs from law enforcement, child protection services, help lines, and relevant regulatory bodies. The Committee further recommends that the Government should establish an integrated national COP digital platform to centralise reporting, guidance, and coordination across schools, ministries, and relevant institutions to improve prevention, response, and information sharing.

2.3.9 Child Online Protection Gaps in Rural Areas

The Committee observes that COP in rural areas remains underdeveloped and insufficiently prioritised, largely due to prevailing assumptions that children in these communities have limited access to mobile phones and the internet. This has resulted in

gaps in prevention, awareness, detection, and reporting mechanisms, as well as weak integration of rural contexts into national COP strategies and data systems.

In this regard, the Committee recommends that COP measures be explicitly extended to rural and hard-to-reach areas through targeted prevention, awareness, and reporting interventions. This should include strengthening community-based detection and referral mechanisms, integrating rural data into national child online protection systems, and ensuring that schools, health facilities, and community structures in rural areas are incorporated into national online safety strategies.

2.3.10 Capacity Building for Emerging Digital Risks

The Committee observes that rapid technological advancements and evolving online risks continue to outpace the capacity of key stakeholders involved in COP, with limited technical skills and institutional readiness undermining effective digital investigations, evidence handling, and child-sensitive justice processes.

In this regard, the Committee recommends that the Government should strengthen institutional capacity through specialised training for law enforcement officers, prosecutors, and members of the judiciary on digital investigations and child-sensitive case handling, supported by appropriate technological tools for the Zambia Police Service's Cyber Unit and Child Protection Unit to enhance effective responses to online offences involving children.

2.3.11 Sustainable Financing for Child Online Protection

The Committee observes that insufficient funding continues to limit the implementation of COP interventions, which have restricted technological safeguards, capacity-building, and awareness efforts. While the National Child Online Protection Strategy (2025–2029), supported by cooperating partners, provides a comprehensive framework, its estimated budget of US$1.8 million remains insufficient to ensure nationwide coverage, particularly in rural and hard-to-reach areas.

In this regard, the Committee recommends that the Government should strengthen domestic financing by establishing a dedicated budget line for COP under the Ministry of Technology and Science, and ZICTA to support sustained implementation. The Committee further recommends that the Government should explore sustainable financing mechanisms, including structured private sector contributions to create a stable local funding stream and ensure continuity of reporting systems, digital literacy initiatives, and awareness programmes.

PART II

3.0 ACTION-TAKEN REPORT ON REPORT OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES FOR THE FOURTH SESSION OF THE THIRTEENTH NATIONAL ASSEMBLY

3.1 REVIEW OF DIGITAL MIGRATION IN ZAMBIA

3.1.1 Multisectoral Solutions

The Committee observed that the implementation of digital migration needed to be pursued through a coordinated and consultative multi-stakeholder approach. In this regard, the Committee recommended that the Ministry of Information and Media engage in comprehensive discussions with Cabinet Office; the Ministry of Finance and National Planning; the Ministry of Infrastructure, Housing and Urban Development; StarTimes Software Technology Company Limited; and other relevant stakeholders. These discussions were aimed at reaching a mutual understanding of the cost implications and agreements on the way forward for completing the remaining components of the Digital Migration Project.

Executive's Response

The Executive, in the Action-Taken Report, submitted that the Government was engaging with other relevant institutions around the resumption and finalisation of the Digital Migration Process. However, the project could not commence due to the country's fiscal constraints. However, the Ministry was advised to consider including the project in the 2026 Medium-Term Expenditure Framework (MTEF) and that the project be executed in a phased manner. The Ministry was, therefore, engaging the contractor to determine their willingness to proceed under the proposed timeline. However, the engagement had not progressed much due to the non-availability of funds, which was the major factor preventing the resumption of the works.

Committee's Observations and Recommendations

The Committee expresses concern that there is still no resolution to the Digital Migration Project. The Committee will await a progress report on the inclusion of the project in the 2026 Medium-Term Expenditure Framework (MTEF) and its execution in a phased manner.

3.1.2 Repayment of Digital Migration Loan

The Committee in the previous Session recommended that the Government assume full responsibility for repaying the loan allocated to ZNBC for the Digital Migration Project. This was due to the Corporation's limited financial capacity, which undermined its sustainability and hampered its ability to effectively deliver its public service mandate.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that in 2017, the Government of Zambia secured financing from the Export-Import Bank of China amounting to US$232.18 million for the Digital Terrestrial Migration Project, alongside a US$40.97 million supplier credit from StarTimes, both of which were on-lent to ZNBC and StarTimes as end-users. Of the EXIM Bank loan, only US$192.73 million was disbursed, with the remaining US$39.45 million cancelled due to delays in debt servicing after 2020, while the supplier credit was fully disbursed. Although ZNBC was expected to meet repayment obligations, the liability ultimately rested with the Treasury. The loan has since been restructured, repayments have resumed, and the Treasury plans to re-engage stakeholders to agree on a revised repayment plan.

Committee's Observations and Recommendations

The Committee resolves to await a progress report on re-engaging the parties to agree on a new repayment plan as prescribed in the Public Debt Management Act.

3.1.3 Establishment of a Converged Regulator

The Committee recommended that the Government should consider converging the IBA and ZICTA to create a single regulator, with a single forward-looking vision for the entire ICT sector.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that the Government would consider converging the IBA and ZICTA to create a single regulator, with a single forward-looking vision for the entire ICT sector. It would, therefore, engage related stakeholders to discuss the recommendations.

Committee's Observations and Recommendations

The Committee, in noting the submission, resolves to await a progress report on the engagements regarding converging the IBA and ZICTA to create a single regulator.

3.1.4 Local Content Development

The Committee in the previous Session recommended that the Government should strengthen the enforcement and monitoring of the 35 per cent local content requirement by establishing clear regulatory mechanisms. Additionally, the Committee recommended that the Government, through the Ministry of Information and Media, should actualise the establishment of the Content Development Fund to finance local content development. This would help create employment and ensure optimal utilisation of channels.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that the IBA Bill had provisions that empowered inspectors of the authority to monitor and ensure that 35 per cent of content was local in line with the digital migration policy. Since the provision was stipulated in the law, the authority would be in a position to enforce and ensure compliance.

Committee's Observations and Recommendations

The Committee, in noting the submission, resolves to await a progress report on the establishment of the Content Development Fund to finance local content development.

3.1.5 State of Equipment

The Committee in the previous Session strongly urged the Government, through the Ministry of Finance and National Planning, to urgently secure funds to pay the

outstanding amount owed for completed works, in order to safeguard the country from substantial loss.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that the Government, through the Ministry of Information and Media, had made steps to ensure the resumption and the completion of 10 per cent of the remaining work. Engagement with the Ministry of Finance and National Planning was ongoing, while the Ministry of Information and Media had generated a Cabinet Memorandum for the resumption of the Digital Migration Project for Cabinet approval.

The Committee was further informed that the Treasury was aware of the outstanding bill amounting to US$12.5 million on completed certified interim payment certificates (IPCs). Further, the Executive submitted that this debt was part of the verified stock of arrears and part of the list that the domestic arrears dismantling strategy had captured in the National Budget. The Treasury would endeavour to prioritise and settle this bill in a phased manner.

Committee's Observations and Recommendations

The Committee, in noting the submission, resolves to await a progress report on the outstanding bill amounting to US$12.5 million on completed certified interim payment certificates.

3.2 ZAMBIA'S ICT INFRASTRUCTURE VIS-À-VIS FINANCIAL TECHNOLOGY GROWTH

The Committee made observations and recommendations arising from outstanding issues from the previous Session as outlined below.

3.2.1 Expansion of Network Coverage

The Committee, in the previous Session, resolved to await a progress report on the construction of the sixty-nine greenfield towers in unserved and underserved areas under the Universal Access and Service Fund.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that the project had been optimised from sixty-nine to eighty towers under Universal Access Phase IV and was at contract signing stage. The Committee was further informed that it would be updated on the progress.

Committee's Observations and Recommendations

The Committee will await a progress report on the construction of eighty greenfield towers in unserved and underserved areas under the Universal Access and Service Fund.

3.3 THE ROLE OF THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY IN THE FIGHT AGAINST CYBER CRIMES

3.3.1 Integrated National Cyber Security System

The Committee, in the previous Session, had resolved to await a progress report on the procurement of an Integrated National Cyber Security System.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that following the issuance of the commencement order for the *Cyber Security Act No. 3 of 2025*, the cyber security mandate had moved from ZICTA to the Zambia Cyber Security Agency, which would oversee this activity. The Committee was informed that it would be updated on the progress.

Committee's Observations and Recommendations

The Committee resolves to await a progress report on the procurement of an Integrated National Cyber Security System.

3.3.2 Compliance Monitoring

The Committee, in the previous Session, resolved to await a progress report on the operationalisation of the Office of the Data Protection Commissioner.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that the operationalisation of the Office of the Data Protection Commissioner was on course, with additional staff appointed to strengthen its institutional capacity. With support from the Zambia Data Acceleration Project, funded by the World Bank, the Data Protection Regulations had been developed and completed and were awaiting approval. Furthermore, Cabinet had granted approval in principle for the repeal and replacement of the *Data Protection Act* to strengthen the legal and institutional framework. The revised law would enable the Office of the Data Protection Commissioner to retain a broader mandate in data protection, including the authority to implement standards and undertake physical inspections of ICT infrastructure before issuing licenses to organisations that handled citizens' sensitive data**.**

Committee's Observations and Recommendations

The Committee resolves to await a progress report on the full operationalisation of the Office of the Data Protection Commissioner.

3.3.3 Security Operations Centre

The Committee, in the previous Session, had resolved to await a progress report on the establishment of a Security Operations Centre (SOC) at national level.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that following the issuance of the commencement order for the *Cyber Security Act No. 3 of 2025*, the cyber security mandate had moved from ZICTA to the Zambia Cyber Security Agency, which would oversee this activity. The Committee was informed that it would be updated on the progress.

Committee's Observations and Recommendations

The Committee resolves to await a progress report on the establishment of a Security Operations Centre at national level.

3.3.4 Need for Updated Statistics

The Committee, in the previous Session, resolved to await a progress report on the creation of a centralised database.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that following the issuance of the Commencement Order for the *Cyber Crimes Act No. 4 of 2025*, the mandate for cybercrime fell under the Ministry of Home Affairs and Internal Security, with supporting functions assigned to the Zambia Cyber Security Agency. In addition, an online public portal had been developed and was hosted by ZICTA to capture real-time reported consumer cybercrime complaints for monitoring and reference purposes. The Committee would be updated on the progress.

Committee's Observations and Recommendations

The Committee resolves to await a progress report on the creation of a centralised database.

3.3.5 Amendment of Legislation

The Committee, in the previous Session, had resolved to await a progress report on the review of the *Cyber Security* and *Cyber Crimes Act, No. 2 of 2021* and the *Information and Communication Technologies Act, No. 15 of 2009*.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that the *Cyber Security Act* and the *Cyber Crimes Act* were both promulgated in 2025. With regard to the ICT Act, the Committee was informed that an institutional review had been undertaken and the matter remained a work in progress, with a further impact assessment planned for 2025. The Committee was further informed that it would be updated on the progress.

Committee's Observations and Recommendations

The Committee resolves to await a progress report on the review of the *Information and Communication Technologies Act, No. 15 of 2009.*

3.4 REVIEW OF THE MEDIA SPACE IN ZAMBIA

3.4.1 Zambia Media Council Legislation

The Committee, in the previous Session, urged the Government to provide a timeline for enacting the Zambia Media Council legislation and resolved to await a progress report on the matter.

Executive's Response

The Executive, in the Action-Taken Report, informed the Committee that the Ministry of Information and Media would facilitate the submission of the Zambia Institute of Journalism Bill (formerly the Zambia Media Council legislation) to the Ministry of Justice for drafting. In the process, the Ministry of Justice called for an internal legislation committee meeting; however, some stakeholders were engaged and expressed displeasure with the internal legislation committee meeting. Consequently, the Executive halted the Bill to allow for further clarity on the matter. The Committee would be updated on the next steps.

Committee's Observations and Recommendations

The Committee will await a progress report on the enactment of the Zambia Media Council legislation.

4.0 CONCLUSION

The Committee notes that Zambia has made commendable progress in establishing a strong legal, policy, and institutional framework for COP. The *Cyber Crimes Act No. 4 of 2025* and the National COP Strategy provide a solid foundation, while multi-stakeholder collaboration ensures broad engagement. However, challenges such as limited awareness, enforcement capacity, infrastructure gaps, and rapid technological changes persist. Addressing these requires sustained investment in digital literacy, technical capacity building, ISP co-regulation, and community-level outreach. By implementing the recommended actions and fostering continuous research and innovation, Zambia can create a safer and more empowering online environment for all children.

The Committee, therefore, urges the Executive to give due consideration to the recommendations contained in its Report to advance a safe and secure digital environment for Zambia's children.

Eng. Raphael S Mabenga, MP
CHAIRPERSON

April, 2026
LUSAKA

Appendix I – List of the National Assembly Officials

National Assembly
Mr Charles Haambote, Director (Social Committees)
Mrs Chitalu K Mumba, Deputy Director (Social Committees)
Mr Darius Kunda, Senior Committee Clerk (SC1)
Mr Leon J N Haangala, Committee Clerk
Mrs Rachael M Kanyumbu, Administrative Assistant
Mr Daniel Lupiya, Senior Committee Assistant
Mr Muyembi Kantumoya, Committee Assistant
Ms Taona Chabinga, Committee Assistant
Ms Monde Mataa, Intern

Appendix II – List of Witnesses

Advocacy for Child Justice
Baobab College
ChildFund Zambia
David Kaunda National Technical Secondary School
Independent Schools Association of Zambia
Lifeline Childline Zambia
Ministry of Community Development and Social Services
Ministry of Education
Ministry of Justice
Ministry of Technology and Science
Ministry of Youth, Sport and Arts
Plan International Zambia
Save the Children Zambia
SMART Zambia
TechTrends Zambia
Ubuchingo – Defence for Children Zambia
University of Lusaka – School of Information Technology
University of Zambia– Department of Computer Science & Informatics
World Vision Zambia
Zambia Information and Communication Technologies Authority
Zambia National Education Coalition
Zambia Police – Child Protection Unit