Watoto Watch Network

EXPLORING THE BARRIERS HINDERING EFFECTIVE REPORTING OF ONLINE CHILD SAFETY ISSUES IN KENYA

FINAL RESEARCH REPORT

Watoto Watch Network

14th November 2025

EXPLORING THE BARRIERS HINDERING EFFECTIVE REPORTING OF ONLINE CHILD SAFETY ISSUES IN KENYA

2025

Author:
AICS Consulting

https://watotowatchnetwork.org

Table of Contents

Acknowledgements

This study was undertaken with the support of InterNews Europe, whose funding and strategic guidance through the InterNews Kenya office enabled its successful completion. We also acknowledge the valuable collaboration of Internet Without Borders as implementation partners and AICS Consulting as research partners throughout the process.

We extend our appreciation to the institutional actors, NGO representatives, educators, and community practitioners who participated in the Key Informant Interviews and contributed essential insights into Kenya's online child-safety reporting systems. Their perspectives informed the depth and accuracy of the analysis.

We further thank the parents, caregivers, and children who participated in the Focus Group Discussions and usability walkthroughs. Their willingness to engage with sensitive topics provided critical context and strengthened the practical relevance of the findings.

We acknowledge the contributions of the project team whose coordination, methodological input, and fieldwork leadership ensured rigorous data collection and smooth implementation.

Finally, we appreciate all stakeholders who took part in the validation workshop and offered constructive feedback that refined the conclusions and enhanced the policy and programmatic recommendations presented in this report.

Executive Summary

The study "Exploring the Barriers Hindering Effective Reporting of Online Child Safety Issues in Kenya" explores the factors that limit effective reporting of online child abuse, grooming, cyberbullying, sexual exploitation, and related digital harms. Conducted under the Kenya Safe and Inclusive Digital Space (KenSafeSpace) Project led by the Bloggers Association of Kenya (BAKE) and Watoto Watch Network, with technical support from AICS Consulting Ltd, the study aimed to identify the social, structural, and technological barriers that inhibit children, parents, caregivers, and institutions from reporting online child safety incidents.

Drawing from key informant interviews, focus group discussions, usability walkthroughs and an extensive review of national child protection frameworks, the study reveals how social, structural and technological barriers impact the identification and response to online harm by children, caregivers, teachers and institutions. The findings highlight a disconnect between policy ambition and lived reality, where reporting pathways exist on paper but are often inaccessible, misunderstood, or mistrusted by the very communities they're designed to serve.

The major findings of the study are presented under three domains. Socially, a lack of awareness, stigma and distrust of formal institutions is the biggest deterrent. Children often do not recognize online harm or have low confidence in navigating mechanisms for reporting. Parents and caregivers face the problem of guiding children due to a lack of digital literacy or fear of being blamed and facing community judgement. Cultural norms that silence conversations around sexuality or abuse also contribute to the underreporting of incidents even, especially when informal settlements or traditional systems of resolving disputes are preferred.

Structurally, Kenya's child protection ecosystem is characterized by fragmented mandates, lack of coordination and uneven institutional capacity. Agencies such as the police, helplines, schools and community structures work in relative isolation, referrals are inconsistent and follow-up is inconsistent. Schools, which are often the first point of disclosure for children, have no standardized approaches to safeguarding and often use manual, undocumented approaches. Helplines and cybercrime reporting mechanisms do not have unified case tracking mechanisms, and police units are resource constrained and lack specialized skills, especially in handling and managing digital pieces of evidence. These structural weaknesses heighten public doubt and lead to a cycle where underreporting becomes a symptom and result of gaps within the institutional system.

Technologically, the digital divide has a strong influence upon who can access and trust online reporting mechanisms. Many reporting tools require smartphones, data bundles, or English-language proficiency, limiting their accessibility to children and caregivers in low-income or rural settings. On mainstream social media platforms, the interfaces for reporting are often confusing, lengthy, or linked to personal accounts, undermining the right to anonymity. Limited vernacular content moderation means harmful content in local languages frequently goes undetected. In addition, interoperability between digital systems is still weak and reports are not efficiently shared or tracked across agencies.

Overall, the findings show that effective reporting is less about the number of available platforms and more about whether these platforms are trusted, child-friendly, well-coordinated, and backed by institutions capable of timely action. The study concludes that without strong structural reforms especially around enforcement, data systems and coordinated response, investments in awareness campaigns or new technologies will make limited impact. Strengthening institutional credibility, making reporting processes simpler and incorporating child-centered design principles are thus key components to build a safer digital environment for Kenyan children.

Purpose and Methodology

The research used a qualitative design to explore the social, structural, and technological barriers shaping reporting behaviors. Data were collected through Key Informant Interviews with civil society actors, teachers, parents, community leaders, and law enforcement, as well as Focus Group Discussions with children and caregivers across Nairobi County. Findings were compared with national child protection frameworks such as the Children Act (2022), the National Plan of Action to Tackle Online Child Sexual Exploitation and Abuse (2022–2026), and research by Internews (2024), Etyang (2025), and Ochieng (2023). All processes complied with NACOSTI ethics, informed consent, and data protection standards.

Key Findings

The study revealed three interrelated domains of barriers:

1. Social Challenges

Cultural stigma, fear of exposure, and mistrust of institutions discourage victims and caregivers from seeking help. Many children are unaware of reporting mechanisms or fear being blamed, while parents often lack the digital literacy to identify or respond to online exploitation. Misinformation, silence, and fear of social judgment perpetuate underreporting.

2. Structural Challenges

Although Kenya has strong legal and policy frameworks, institutional response systems are fragmented and under-resourced. Helplines, police, schools, and community structures operate in silos, weakening referrals and follow-up. Schools lack functional safeguarding protocols, and frontline responders have limited capacity to manage digital harms. Critically, the ability of institutions to enforce laws and provide timely feedback remains weak, further reducing public trust.

3. Technological Challenges

Technological barriers include poor connectivity, non-anonymous reporting platforms, limited vernacular content moderation, and weak interoperability across reporting systems. The digital divide disproportionately affects rural and low-income areas, restricting access to safe reporting channels for many children and families.

High-Level Recommendations

Social Domain: Scale up digital literacy and awareness campaigns for parents, teachers, and children; foster safe community dialogue on online risks; and integrate online safety education in schools.

Structural Domain: Strengthen coordination among agencies through the Child Protection Information Management System (CPIMS); allocate sustainable funding; and embed online child protection training in teacher and police curricula. Strengthening the enforcement of child online protection laws (which includes timely investigation, prosecution, and feedback) is essential to restoring public trust.

Technological Domain: Develop localized and anonymous reporting platforms, expand digital infrastructure in schools and communities, and invest in local language-sensitive moderation and interoperable national systems.

Overall, the study concludes that meaningful progress requires prioritizing structural reforms, particularly the ability of institutions to enforce laws, investigate cases, and ensure accountability. Without strong enforcement and coordinated institutional response, investments in awareness and technology will have limited impact. A trusted, integrated, and enforceable protection system is therefore central to ensuring that every child in Kenya can report online harm safely, confidently, and with assurance that action will follow.

Introduction

2.1 Background

Digital Connectivity and the Changing Childhood in Kenya

Kenya's digital landscape has undergone a profound transformation over the past decade, reshaping how children learn, communicate, and participate in society. By early 2024, the country had 22.7 million internet users, representing 40.8 percent internet penetration, while mobile subscriptions exceeded 66 million, equivalent to 118 percent of the population thus indicating multiple connections per person (DataReportal, 2024). The Communications Authority of Kenya (2025) reports that mobile broadband subscriptions have surpassed 58 million, with smartphone penetration above 80 percent, positioning Kenya as one of Africa's most digitally connected nations.

For children, this connectivity offers new opportunities for education, self-expression, and civic engagement, particularly through e-learning platforms and social media. However, as Kenya's young population increasingly moves online, exposure to cyberbullying, online grooming, sextortion, sexual exploitation, and trafficking through digital channels has also escalated (ECPAT International, 2018). The rapid digitalization of schools, social networks, and gaming environments which are often introduced without adequate safeguards, has expanded children's vulnerability to Online Child Sexual Exploitation and Abuse (OCSEA).

> "However, as Kenya's young population increasingly moves online, exposure to cyberbullying, online grooming, sextortion, sexual exploitation, and trafficking through digital channels has also escalated (ECPAT International, 2018).

Kenya's digital landscape has undergone a profound transformation over the past decade, reshaping how children learn, communicate, and participate in society. By early 2024, the country had 22.7 million internet users, representing 40.8 percent internet penetration, while mobile subscriptions exceeded 66 million, equivalent to 118 percent of the population thus indicating multiple connections per person (DataReportal, 2024). The Communications Authority of Kenya (2025) reports that mobile broadband subscriptions have surpassed 58 million, with smartphone penetration above 80 percent, positioning Kenya as one of Africa's most digitally connected nations.

For children, this connectivity offers new opportunities for education, self-expression, and civic engagement, particularly through e-learning platforms and social media. However, as Kenya's young population increasingly moves online, exposure to cyberbullying, online grooming, sextortion, sexual exploitation, and trafficking through digital channels has also escalated (ECPAT International, 2018). The rapid digitalization of schools, social networks, and gaming environments which are often introduced without adequate safeguards, has expanded children's vulnerability to Online Child Sexual Exploitation and Abuse (OCSEA).

During the validation meeting for this study, stakeholders from Watoto Watch Network (WWN) and AICS Consulting Ltd emphasized that while children are deeply embedded in the digital space, their awareness of risks and of where to seek help has not kept pace. As the WWN Director noted, the motivation for commissioning this research emerged from a practical dilemma: children were disclosing disturbing online experiences to programme staff, yet they were not using formal reporting platforms. The central question became whether this was primarily a problem of low awareness, weak system performance, or both.

Emerging Risks and the Reality of Under-Reporting

Existing evidence points to a stark gap between children's lived experiences of online harm and formal reporting data. The Disrupting Harm in Kenya study (ECPAT, INTERPOL & UNICEF, 2021) found that around 6 percent of internet-using children aged 12–17 had shared naked images or videos of themselves in the preceding year, and about one-third of children subjected to OCSEA had told nobody. Administrative data from the Anti-Human Trafficking and Child Protection Unit (AHTCPU) of the Kenya National Police Service show reported OCSEA cases rising from 3,160 in 2018 to 4,133 in 2019, while "CyberTips" concerning suspected child sexual exploitation received through the National Center for Missing and Exploited Children (NCMEC) reached more than 16,000 in some years.

In the validation discussion, partners highlighted the contrast between these large volumes of incoming image-based abuse alerts and the relatively low number of cases that appear in Kenyan law enforcement and child protection statistics. They noted that on average, about 150 reports of images and videos involving Kenyan children are flagged per day through NCMEC, yet national systems do not reflect a comparable scale of formal complaints, investigations or convictions. This reinforces earlier research from Nairobi's informal settlements of Kibera and Mathare, which shows that children often access the internet unsupervised through shared devices and rarely disclose online harm to formal authorities (Ochieng, 2023).

THEY NOTED THAT ON AVERAGE, ABOUT 150 REPORTS OF IMAGES AND VIDEOS INVOLVING KENYAN CHILDREN ARE FLAGGED PER DAY THROUGH NCMEC

Similar trends are observed regionally. Studies across Eastern and Southern Africa document frequent exposure to sexual imagery, unsolicited contact, and cyberbullying, but also high levels of normalization and silence (ChildFund & African Child Policy Forum, 2024). Parental and caregiver capacity to respond remains limited; only about one-third of Kenyan parents report ever discussing online safety with their children (Etyang, 2025), and economic inequalities and device-sharing practices further constrain supervision.

Policy, Legislative, and Institutional Context

Kenya has taken important steps to address these risks through legal and policy instruments such as the Children Act (2022), the Computer Misuse and Cybercrimes Act (2018), and the National Plan of Action to Tackle OCSEA (2022–2026) (National Council for Children's Services, 2022). These frameworks are broadly aligned with global guidance, including the ITU Child Online Protection Guidelines (2023) and UNICEF's Global Strategy for Online Safety (2021).

However, as discussed during the validation meeting, implementation gaps remain significant. Agencies such as the Directorate of Criminal Investigations (DCI), the Communications Authority (CA), the Office of the Data Protection Commissioner (ODPC) and the State Department for Children's Services (SDCS) hold partial mandates over child online protection, but information sharing is inconsistent and often project-based. Participants noted that while the CA annual report includes an annex on reporting cybercrime and child online protection incidents, there is limited transparent, disaggregated data on trends in child-related reports or on the performance of campaigns such as "Be the COP." The Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC) tracks cyber incidents, yet its quarterly reports do not clearly identify cases involving children.

Frontline actors, including teachers, social workers and police officers, often lack specialised training on digital evidence, survivor-centred approaches, and online exploitation patterns. During the validation session, stakeholders also raised concerns that some AHTCPU officers receive cases directly to their personal phones, creating legal and data protection risks, and that many cases are still settled informally at community level without entering formal systems.

Digital Governance and Civil-Society Mobilization

In response to these challenges, the Kenya Safe and Inclusive Digital Space (KenSafeSpace) project, funded by the European Union, was established to strengthen human rights–based digital governance and support a safe, inclusive digital environment. The consortium is led by the Bloggers Association of Kenya (BAKE) in partnership with Internews, KICTANet, Internet Without Borders, Tribeless Youth, Mzalendo Trust and Watoto Watch Network (AICS Consulting Ltd., 2025).

Within this collaborative framework, Watoto Watch Network has emerged as a leading civil-society actor on child online safety through long-standing programmes with schools, churches and community groups, nationwide Safer Internet Day campaigns, and the Child Tech Counties Consortium, which engages county governments on child-centered digital policies. During the validation meeting, AICS Consulting highlighted that this study builds on earlier efforts to develop digital safety materials approved by the Kenya Institute of Curriculum Development (KICD), and that findings from the present research are expected to inform future iterations of those tools.

Persistent Gaps in Reporting and Accountability

Despite the proliferation of reporting avenues (including social media reporting features, the KE-CIRT reporting app, the Internet Watch Foundation (IWF) portal, the DCI toll-free line, the 116 Child Helpline and community child protection structures) reporting rates for online child safety violations remain low (Ndemo & Munyuwiny, 2018). Both the literature and the validation discussions underscored that children tend to disclose to people they know (such as parents, friends or teachers) rather than to

helplines or the police, and that adults themselves are often unclear about which platform to use and how escalation should work.

The National Plan of Action to Tackle OCSEA in Kenya (2022–2026) recognizes that reporting procedures from communities to service providers are not well understood, and that children who do report may feel guilty or unsupported in coping with trauma. Equality Now's factsheet on online sexual exploitation in Kenya similarly notes that incomplete and fragmented reporting makes it difficult to build an accurate statistical picture.

Internationally, the OECD (2020) and the Global Partnership to End Violence Against Children (2023) identify under-reporting as a global bottleneck driven by stigma, privacy concerns, mistrust of authorities, and weak feedback loops. In sub-Saharan Africa, fragmented mandates and low investment in digital child protection systems further constrain effective reporting (ACPF, 2024).

In Kenya, these dynamics are reinforced by intersecting social, structural and technological barriers. Socially, stigma, shame and self-blame discourage disclosure; structurally, weak inter-agency coordination, limited resourcing and slow justice processes undermine confidence; technologically, low digital literacy, poor interface design and lack of transparency about data handling discourage the use of online tools.

2.2 Problem Statement

Despite notable progress in Kenya's legal and policy environment, underreporting of online child safety violations remains one of the most persistent weaknesses within the national child protection system. The country has established multiple mechanisms ranging from the 116 Child Helpline to cybercrime reporting units, and social media flagging tools. Despite this, a profound gap persists between the prevalence of online harm and the rate of formal reporting (Etyang, 2025). Recent analyses highlight that many children and caregivers experience online risks such as grooming, sextortion, and cyberbullying but rarely report them through official channels. In most instances, victims resort to silence, self-censorship, or informal dispute resolution due to fear of stigma, lack of confidence in institutional response, or ignorance of available mechanisms (Ochieng, 2023).

This pattern of silence is not unique to Kenya. Global and regional research by ECPAT International (2018) and the Global Partnership to End Violence Against Children (2023) shows that underreporting is the norm rather than the exception, even where strong legal frameworks exist. Across Africa, fewer than 20 percent of children who experience online sexual exploitation or abuse disclose it to a trusted adult or authority, and fewer than 10 percent make a formal report (ChildFund & ACPF, 2024). In Kenya, similar dynamics are observed: parents and teachers may notice behavioral changes but avoid pursuing formal redress due to cultural taboos, lengthy justice processes, and a perception that online abuse is "less real" than physical harm (Ndemo & Munyuwiny, 2018).

The Internews (2024) assessment of Kenya's digital information ecosystem identifies a widespread sense of "digital helplessness," where citizens feel overwhelmed by online threats yet uncertain about how or where to seek help. It documents low trust in digital institutions, confusion over reporting procedures, and fragmented communication between service providers. Users often encounter multiple platforms which include helplines, mobile applications, social media reporting features. Nevertheless, these systems are disconnected, poorly publicized, and non-interoperable and as a result, victims are left unsure of which channel guarantees confidentiality or action, while agencies duplicate or ignore reports due to weak coordination and absence of shared databases.

Further complicating the landscape is the evolving nature of digital threats. Kenya's data protection and cybersecurity frameworks have not fully adapted to emerging risks such as AI-generated child sexual abuse material, deepfakes, identity manipulation, and cross-border trafficking rings (Internews, 2024; OECD, 2020). The inability to trace perpetrators operating through encrypted networks or offshore platforms further erodes confidence in formal systems. A 2023 ITU review

warned that without investments in forensic capacity and AI-governance mechanisms, African countries risk falling behind in identifying and prosecuting online exploitation (ITU, 2023).

At the community level, the problem manifests differently. Schools, faith institutions, and community leaders remain critical frontline actors for detecting and responding to child abuse, yet their reporting systems are largely offline, informal, and poorly linked with national databases. Teachers often rely on personal judgment, while school counsellors lack digital tools to escalate reports effectively. Similarly, chiefs and local administrators collect anecdotal complaints but have limited capacity to refer them through electronic systems or to the police. This fragmentation leaves children, especially those in rural and low-income areas, effectively voiceless within Kenya's digital protection framework.

Cultural attitudes further entrench underreporting. In some Kenyan communities, online exploitation is viewed as a private family matter, and victims are often blamed for attracting online attention (Ochieng, 2023). Families may prefer to negotiate compensation or informal settlements rather than engage formal institutions perceived as slow or corrupt. Among adolescents, peer shaming and fear of reputational damage on social media discourage disclosure. These psychosocial barriers intersect with structural and technological constraints to create a perfect storm of silence and inaction.

At the institutional level, weak coordination among government agencies undermines case management. The Directorate of Criminal Investigations (DCI), National Council for Children's Services (NCCS), Communications Authority, and the Office of the Data Protection Commissioner all hold partial mandates over child online protection, yet information sharing is inconsistent and often project-based (CIPESA, 2025). The absence of a centralized reporting database or integrated referral mechanism means that agencies may record cases independently, producing fragmented data and limiting accountability.

Moreover, limited resourcing and human capacity contribute to systemic inertia. Police officers, prosecutors, and child protection officers often lack specialized training to handle digital evidence or provide survivor-centered responses. According to the Disrupting Harm study (ECPAT, INTERPOL & UNICEF, 2021), delays in evidence collection and the inability to retrieve digital proof frequently result in case collapse. The same study found that survivors who do report often receive inadequate follow-up, reinforcing public perception that reporting yields no tangible results.

These factors have produced what Internews (2024) describes as a "trust deficit" in digital governance. Citizens may view reporting systems as symbolic rather than functional as they are visible on paper but ineffective in practice. Without trusted, accessible, and responsive mechanisms, Kenya's otherwise progressive digital safety frameworks fail to reach the most vulnerable populations, particularly children in rural and marginalized settings.

Hence, this study responds to an urgent need for a grounded, evidence-based analysis of the barriers hindering effective reporting of online child safety issues across multiple pathways which mainly include online platforms, helplines, school systems, legal channels, and community structures. By examining these barriers through the social, structural, and technological domains, the study aims to uncover how social norms, institutional weaknesses, and digital inequities collectively silence children's voices in Kenya's online safety ecosystem.

"

By examining these barriers through the social, structural, and technological domains, the study aims to uncover how social norms, institutional weaknesses, and digital inequities collectively silence children's voices in Kenya's online safety ecosystem.

2.3 Purpose and significance of the study

Against this backdrop, the Watoto Watch Network study, implemented under the KenSafeSpace project with technical support from Internews, investigates the barriers hindering effective reporting of online child safety issues in Kenya. The study adopts an integrated lens that examines how social, structural and technological factors influence reporting behaviour across five key pathways: online platforms, helplines and SMS services, school-based mechanisms, police and formal legal systems, and community or informal structures.

As highlighted by the research team during the validation workshop, the focus is not only on online platforms themselves, but on the full continuum from digital entry points to offline institutions where cases are ultimately handled. The findings aim to contribute evidence for strengthening implementation of the National Plan of Action to Tackle OCSEA (2022–2026) and to support alignment with the African Union Digital Transformation Strategy (2020–2030), which calls for safe and empowering digital ecosystems for children. Ultimately, the study seeks to inform national policy, enhance cross-sector collaboration and support the design of trusted, accessible and child-centred reporting systems so that Kenya's digital progress advances, rather than undermines, children's rights and well-being.

2.4 Study Purpose and Objectives

The overarching purpose of this study is to examine the barriers hindering effective reporting of online child safety issues in Kenya, particularly in relation to grooming, cyberbullying, sextortion, and sexual exploitation. It aims to generate evidence-based insights that inform the design of accessible, trustworthy, and responsive child protection systems capable of adapting to Kenya's digital transformation.

The specific objectives are to:

1. Identify and analyze the social, structural, and technological barriers that prevent children, parents, caregivers, teachers, and community actors from reporting online abuse and exploitation.
2. Assess how these barriers manifest differently across five reporting pathways:
    a. Online platforms (web forms, mobile apps, in-platform reporting on social media);
    b. Helplines and SMS services (e.g., the national 116 helpline);
    c. School-based reporting mechanisms (teachers, counselors, safeguarding focal points);
    d. Police and formal legal systems (including the DCI Cyber Unit and children's officers);
    e. Community and informal mechanisms (trusted adults, chiefs, faith-based networks, and peer groups).
3. Provide policy and programmatic recommendations to strengthen coordination, capacity, and trust within Kenya's child protection reporting ecosystem.

These objectives reflect the recognition that reporting is not merely a technical function but a relational and social process that depends on awareness, trust, institutional credibility, and system responsiveness.

2.4 Rationale and Significance

This study is being undertaken at a critical juncture in Kenya's digital evolution. The COVID-19 pandemic accelerated digital learning and remote communication, dramatically increasing children's screen time and exposure to online risks (Etyang, 2025, p. 39). At the same time, the proliferation of smartphones and social media platforms has outpaced efforts to embed safety-by-design principles or parental controls that are accessible and culturally relevant. The 2023 ECPAT International report emphasizes that low- and middle-income countries like Kenya face a dual challenge of growing connectivity and limited regulatory enforcement, which together facilitate the spread of CSAM and grooming networks (ECPAT International, 2018, pp. 55–63).

Within this context, Watoto Watch Network's leadership under the KenSafeSpace project provides an opportunity to bridge policy, advocacy, and community-level action. The organization's ongoing initiatives such as the Child Tech Counties Consortium which demonstrates the importance of county-level ownership in addressing digital safety. However, these initiatives also reveal the systemic fragmentation that persists between national child protection agencies, telecommunications authorities, and grassroots organizations. At the national level, it aligns with the Kenya National ICT Policy (2022) and the National Plan of Action on Online Child Sexual Exploitation and Abuse (2022–2026), which call for stronger cross-sectoral mechanisms for prevention and response. At the global level, it complements the ITU Child Online Protection (COP) Framework, which identifies reporting and response systems as a key pillar of national digital safety infrastructure (International Telecommunication Union, 2023).

- The findings are expected to inform multi-stakeholder initiatives aimed at:
- Enhancing digital literacy among children, parents, and educators;
- Strengthening capacity of helpline and police staff;
- Improving coordination between online platforms and law enforcement; and
- Embedding digital safeguarding protocols in schools and community programs.

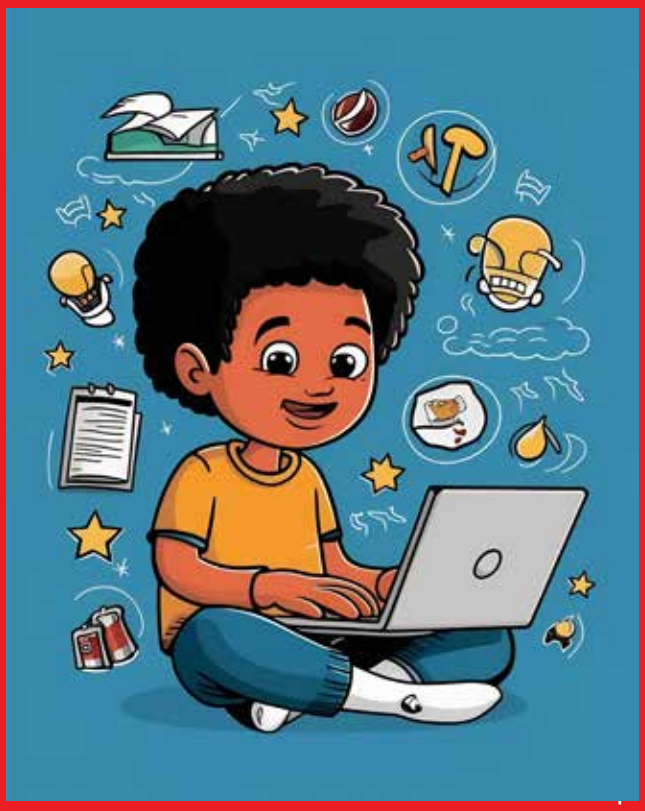
2.5 Scope and Expected Contribution

The scope of this research extends beyond identifying barriers; it aims to connect the lived experiences of children and caregivers with systemic and technological realities. The study draws data from diverse respondents including children, parents, teachers, NGOs, and government representatives. It captures both the demand side (willingness and ability to report) and the supply side (institutional readiness to respond).

By systematically categorizing barriers into social, structural, and technological domains, the study provides a clear analytic framework for understanding Kenya's OCSEA reporting ecosystem. Its findings will contribute to the design of national campaigns, helpline reforms, school safeguarding programs, and platform accountability measures thereby advancing Kenya's journey toward a safe, inclusive, and child-centered digital environment.

Conceptual and Theoretical Framework

This qualitative study is anchored in two complementary frameworks—the Social-Ecological Model (SEM) and the Technology Acceptance and Trust Model (TATM)—to interpret the complex social, institutional, and technological factors influencing whether and how children, caregivers, and frontline actors report online child safety concerns in Kenya. These frameworks guide the thematic analysis of interview and focus group data, enabling a grounded understanding of how lived experiences, perceptions, and contextual realities shape reporting behavior.



Social-Ecological Model (SEM)

The SEM provides a multilayered lens for interpreting qualitative insights by recognizing that children's decisions to disclose online harm are shaped by nested social environments rather than isolated individual choices. Originating from Bronfenbrenner's ecological theory, the model emphasizes five interconnected levels—individual, interpersonal, community, institutional, and societal—which influence behaviors and outcomes.

At the individual level, qualitative narratives reveal that children's recognition of online harm depends on their digital literacy, emotional readiness, and confidence in seeking help. Interpersonally, children in FGDs frequently referred to peers, caregivers, and teachers as their primary sources of support, illustrating how trust and relational safety strongly mediate disclosure. At the community level, cultural taboos surrounding sexuality, concerns about family reputation, and normalized silence emerged as recurring barriers, echoing regional findings by CIPESA (2025) and ChildFund–ACPF (2024).

Institutionally, teachers, police, and child protection officers shape children's and caregivers' willingness to report through their attitudes, responsiveness, and training. Finally, societal factors—including laws, public awareness campaigns, and national digital norms—create the overarching climate in which reporting is encouraged, discouraged, or rendered confusing.

In qualitative research on violence against children, ecological models are widely used to explain disclosure patterns because they capture the interplay of personal, relational, and system-level influences (WHO, 2020; UNICEF, 2021). In this study, SEM enables a nuanced reading of how stigma, mistrust, social norms, and institutional weaknesses collectively produce low levels of formal reporting.

> "AT THE INDIVIDUAL LEVEL, QUALITATIVE NARRATIVES REVEAL THAT CHILDREN'S RECOGNITION OF ONLINE HARM DEPENDS ON THEIR DIGITAL LITERACY, EMOTIONAL READINESS, AND CONFIDENCE IN SEEKING HELP.

Technology Acceptance and Trust Model (TATM)

While the SEM contextualizes social and institutional influences, the Technology Acceptance and Trust Model (TATM) helps interpret qualitative insights related to digital reporting systems. The TATM builds on the Technology Acceptance Model (TAM) but incorporates additional components essential to child protection: perceived usefulness, perceived ease of use, trust, and privacy assurance.

Qualitative data highlight that children and adults assess reporting platforms not only based on functionality but also on whether they feel safe using them. Many described online systems as "too complicated," "requiring personal details," or "risky because they can expose you." Such perceptions mirror global evidence that trust deficits (especially fears of data misuse or retaliation) significantly decrease technology uptake (OECD, 2020; Internews, 2024).

Qualitative accounts also show that limited digital literacy and prior negative experiences shape how people judge the usability of reporting channels. In several FGDs, participants expressed uncertainty about where digital reports go and whether anyone responds. This reflects weak feedback loops and inconsistent institutional communication.

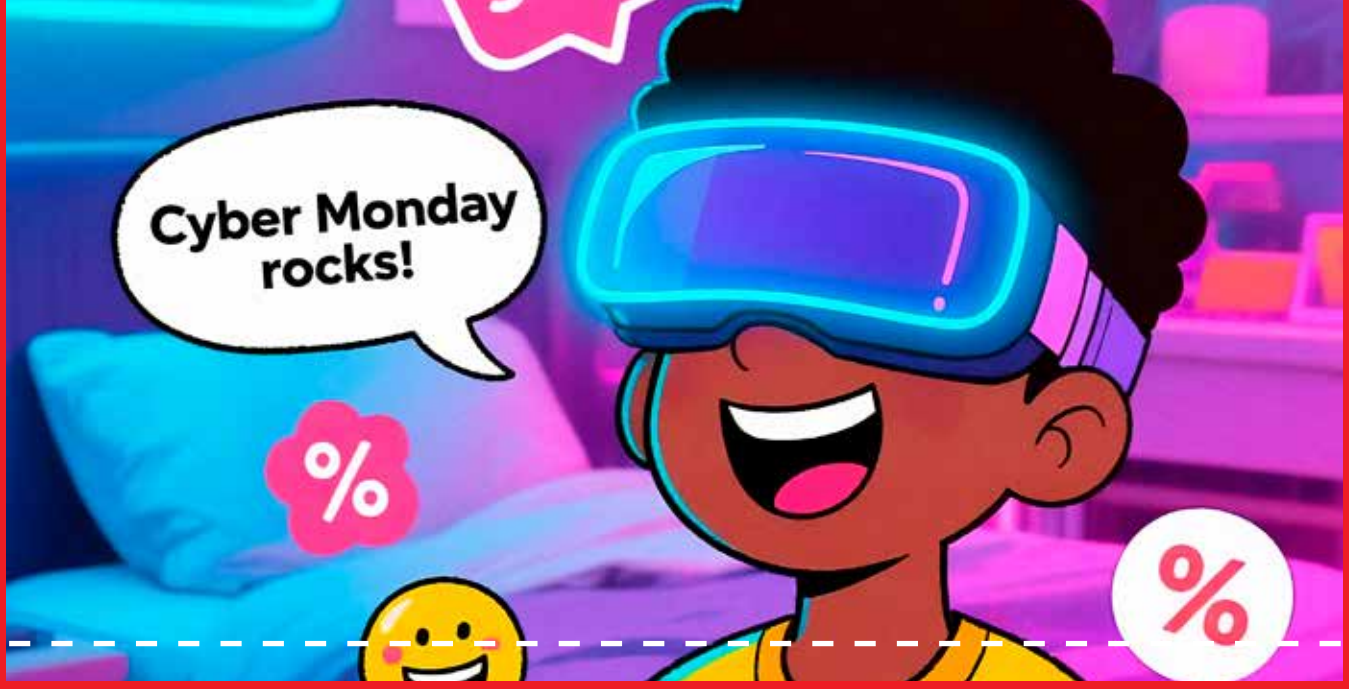
Integrating SEM and TATM

Together, SEM and TATM provide a coherent framework for analyzing qualitative data on reporting behaviors. SEM situates individual decisions within broader social and institutional environments, while TATM captures users' perceptions of digital systems and their trust in them. This combined approach aligns with the ITU COP Framework (2023) and UNICEF's online safety guidelines, both of which emphasize integrated, child-centered systems.

In this study, the combined framework underscores three interconnected pillars that influence reporting of online child safety issues:

1. **Social Enablement**—awareness, stigma reduction, and supportive interpersonal relationships.
2. **Structural Strengthening**—institutional clarity, coordinated referral systems, and frontline capacity.
3. **Technological Trust**—safe, user-friendly, and privacy-assured reporting platforms.

By applying these frameworks to qualitative narratives, the study develops a grounded understanding of why reporting remains limited across online platforms, helplines, schools, police systems, and community mechanisms, and identifies targeted opportunities for strengthening Kenya's child protection ecosystem.



Methodology

4.1 Design

The study adopts a mixed-qualitative design, utilizing qualitative elements to generate a comprehensive understanding of the barriers hindering effective online reporting of child safety issues in Kenya. This design was chosen to integrate narrative insights provided by qualitative evidence to offer deeper explanations of perceptions, experiences, and contextual factors influencing reporting behaviors. This qualitative dimension, emphasized through key informant interviews (KIIs), focus group discussions (FGDs), and usability walkthroughs, enables exploration of social, institutional, and technological barriers. Complementary quantitative data derived from structured surveys and desk reviews help map the prevalence of awareness, trust levels, and accessibility of reporting mechanisms among target groups. This design supports triangulation of evidence across different data sources, enhancing both validity and reliability of findings

4.2 Study Site

The research is being conducted in Nairobi County, specifically within Kibera, one of the city's most densely populated informal settlements. The area was purposively selected due to its high digital connectivity juxtaposed with complex social vulnerabilities, offering an ideal setting to investigate both opportunities and barriers in child safety reporting. Kibera hosts diverse populations including children, caregivers, educators, social workers, and law enforcement officers, who interact regularly with digital technologies and institutional protection systems. The study leverages the operational base of Code with Kids, a local organization located at Olympic Estate, Court C, House No. 138, which implements child protection and online safety interventions in collaboration with local communities and institutions. Conducting the study in this setting ensures access to relevant stakeholders, contextual grounding of findings, and feasibility in field coordination

4.3 Participants

The study targets a diverse range of stakeholders engaged in or affected by child online safety mechanisms. The participant categories include:

1. Children and Adolescents (10–17 years): Engaged through FGDs and usability walkthroughs, with groups segmented by age, gender, and disability status. Parental consent and child assent are mandatory for participation.

2. Caregivers and Parents: Representing household perspectives on awareness, trust, and cultural barriers influencing reporting.

3. Teachers and School Administrators: Providing insights into school-based reporting pathways, institutional challenges, and coordination with law enforcement.

4. Law Enforcement Officers and Child Protection Officials: Including police, Department of Children Services staff, and helpline or call-center personnel responsible for case management.

5. Civil Society and Community-Based Organizations (CSOs/CBOs): Offering perspectives on grassroots advocacy, social mobilization, and referral mechanisms.

6. Technology and Platform Actors: Representatives from telecom operators, social media platforms, and app developers engaged to assess usability, responsiveness, and data protection practices.

This inclusive approach ensures the perspectives of both service users and institutional actors are represented, reflecting the multidimensional nature of online child safety ecosystems.

4.4 Data Collection

Multiple data collection methods are employed to ensure a rich, triangulated evidence base.

a) Desk Review: An initial desk review mapped the existing landscape of Kenya's child protection reporting mechanisms. It examined national policies, legislative frameworks, helpline protocols, and prior assessments by government and non-state actors. This review provided baseline information on institutional capacities, digital platforms, and systemic gaps related to child online safety.

b) Surveys: Structured questionnaires were used to gather quantitative data from children, parents, and teachers on their awareness, trust, and usage of reporting mechanisms. The surveys were designed to capture both frequency and perceived effectiveness of reporting across demographic subgroups.

c) Key Informant Interviews (KIIs): Thirteen semi-structured KIIs were conducted with child protection officers, law enforcement personnel, helpline managers, teachers, counsellors, and representatives from technology companies. Interviews lasted 40–60 minutes and were conducted virtually or in person, depending on participant availability. They focused on institutional barriers, coordination mechanisms, policy gaps, and digital platform practices.

d) Focus Group Discussions (FGDs): Six FGDs were conducted, each comprising 7–9 participants, representing different groups: children (by age and gender), caregivers, teachers, and community leaders. The discussions explored attitudes toward reporting, perceived risks, and expectations of institutional responses. Participatory facilitation tools such as storytelling and scenario-based exercises were used to enhance engagement, especially among younger participants.

e) Usability Walkthroughs: Between twelve and sixteen participants were engaged in practical usability walkthroughs, during which they were guided through the process of reporting a case using live platforms or helplines. Observers recorded user experiences, barriers encountered, and factors influencing trust or withdrawal from the reporting process. These walkthroughs provided tangible data on accessibility, interface design, and real-time user perceptions.

All qualitative data were transcribed verbatim and analyzed thematically using ATLAS.ti and AI-assisted coding tools.

4.5 Ethical Considerations

The study upholds the highest ethical standards, guided by the Belmont Report (1979) principles of respect for persons, beneficence, and justice, as well as the UN Convention on the Rights of the Child (CRC) and Kenya's Children Act (2022). Ethical approval was obtained from the National Commission for Science, Technology and Innovation (NACOSTI) prior to data collection.

Child Safeguarding:

All sessions involving children were conducted in safe, child-friendly environments, with same-gender facilitators where appropriate. A professional counsellor was on standby during FGDs, and referral pathways to Childline Kenya, Department of Children Services, and local psychosocial service providers were pre-established. Any disclosures of abuse triggered mandatory reporting procedures aligned with national child protection protocols.

Informed Consent and Assent:

Adult participants provided written informed consent prior to participation. For children aged 10–17 years, participation was contingent upon both parental consent and child assent. All forms were written in plain language, and participants were briefed on the voluntary nature of their involvement, with the right to withdraw at any point without consequence.

Confidentiality and Data Security:

Data were pseudonymized and securely stored on encrypted devices accessible only to the Principal Investigator. Identifiers were separated from research data, and all quotations used in reporting were de-identified to prevent traceability. Hard copies of consent forms were kept under lock and key.

Risk Mitigation:

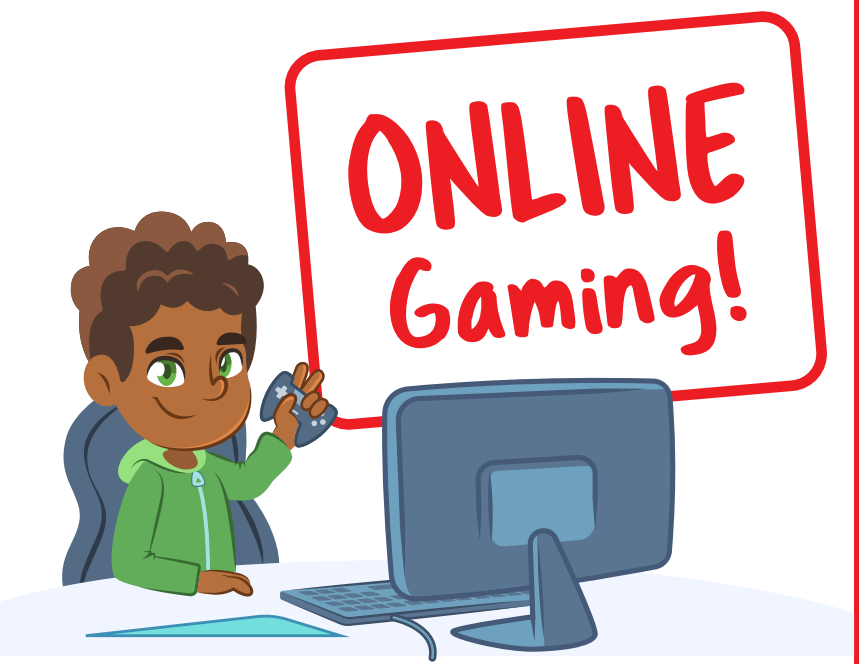
Potential psychological risks, including discomfort from discussing sensitive experiences, were minimized through trauma-informed facilitation, emotional check-ins, and debriefing after each session. No invasive procedures were involved, and no physical, social, or legal risks were anticipated.

Equity and Inclusion:

The sampling strategy prioritized diversity and inclusion, ensuring representation across gender, age, socioeconomic status, and disability. Compensation in the form of refreshments and modest reimbursements for transport were provided to minimize economic barriers to participation.

Accountability and Oversight:

All researchers and field assistants signed AICS Consulting's Child Safeguarding Policy and completed training on ethical conduct in human subjects' research. Continuous monitoring, documentation of field notes, and internal debrief sessions were held to ensure adherence to ethical and methodological standards.



Findings:
Barriers Hindering Effective Reporting of Online Child Safety Issues in Kenya

This section presents findings organized under three broad analytical domains namely social, structural, and technological domains which collectively explain the barriers impeding effective reporting of online child safety issues in Kenya. Data are drawn from Key Informant Interviews (KIIs) with NGOs, parents, and institutional actors, as well as Focus Group Discussions (FGDs) and Usability Walkthrough sessions with children, parents, and educators. The analysis reflects perspectives across five key reporting pathways: online platforms, helplines and SMS services, school-based mechanisms, police and formal legal systems, and community or informal structures.

> "Outside Nairobi, there has been little effort by the government or stakeholders to let children know how to report.

5.1 Social Challenges

Social barriers consistently emerged as the most powerful and deeply rooted obstacles to effective reporting of online child safety concerns. During KIIs, FGDs, and the validation workshop, stakeholders repeatedly emphasized that even when digital tools, helplines, or institutional pathways exist, social attitudes and behaviors ultimately determine whether children and adults use them. Respondents across all categories agreed that unless Kenya addresses these underlying social and cultural dynamics, improvements in technology or institutional processes will have limited impact.

Three cross-cutting themes dominated the analysis: lack of awareness, fear and mistrust, and cultural norms that silence disclosure. Together, these dynamics influence behaviour across every reporting pathway.

5.1.1 Online Platforms

Across all interview groups, there was strong agreement that both children and caregivers lack basic knowledge and confidence about how to use online reporting tools. Awareness is low not only about how to report but also why reporting matters. As one NGO respondent explained, "Outside Nairobi, there has been little effort by the government or stakeholders to let children know how to report" (KII_NGO_4 & KII_NGO_5).

Children confirmed this. In multiple FGDs, they said they often encounter harmful content, but their instinctive response is simply to "block the person or delete the message," because they do not know a trusted adult or platform to report to (FGD_CHD_1).

Validation workshop insights reinforced these findings:

- Many parents lack the digital awareness needed to guide their children.
- Even caregivers with smartphones admitted they rarely understand reporting icons or safety menus.
- Several participants stated that "parents themselves need training before they can help their children."

- Usability walkthrough findings revealed structural usability challenges that reinforce social fears:
- Many users struggled to locate reporting buttons on TikTok, Instagram, and Facebook.
- Reporting menus were described as "too long," "too confusing," or "requiring too much information."
- Some participants felt that the systems "do not let you explain properly what happened."

The fear of exposure remains one of the strongest deterrents. Children worry that their identity might be revealed to peers, parents, or even perpetrators. As one child stated during the usability test, "If I report with my phone, they will know." An institutional respondent summarized: "These systems have gaps that can expose you. I feel unsafe; I'd rather not report" (FGD_INST_1).

Parents share similar mistrust. A mother noted, "I've lost trust in that reporting… when I report issues, they are never handled" (KII_PAR_1). Caregivers also expressed confusion about what constitutes reportable online abuse. One NGO worker said: "Once an abuse happens online, like sharing nude photos, parents often do not know it is abuse" (KII_NGO_2).

The validation workshop introduced an additional nuance: generational digital gaps.

- Urban parents may occasionally discuss cyberbullying.
- Many rural parents still view the internet as "an adult space," leaving children to navigate online harm alone.

5.1.2 Helplines and SMS Services

The national Child Helpline 116 is widely recognized across Kenya due to long-running public campaigns. However, usability and social perceptions significantly undermine its effectiveness. Users described the service as "unreliable," "overwhelmed," or "slow." As one NGO explained: "116 is run by Childline Kenya and is overwhelmed. All reporting channels don't speak to each other; everyone is running their own show" (KII_NGO_2).

Usability walkthrough findings confirmed inconsistent responsiveness:

- Some calls were answered within 6 seconds.
- Others took up to 20 seconds or more.
- Some children were unsure whether they should report "online issues" through the helpline.

A major social concern is lack of anonymity. In many communities, phone numbers are known, making it easy for others to guess who reported. Parents feared backlash, while children feared being blamed. One child said, "If people know you called, you'll be blamed."

During the workshop, participants highlighted that while WhatsApp reporting exists, few users know how it works or whether it ensures privacy.

5.1.3 School-Based Reporting

Schools are deeply trusted by children, yet socially and structurally ill-equipped to manage online child safety reports. NGO informants stressed the disparity: "Kids in informed schools may benefit, but those in rural schools have no idea what reporting looks like" (KII_NGO_4 & KII_NGO_5).

FGDs with children revealed troubling patterns:

- Some teachers blame victims ("It's your fault for using phones").
- Some schools discourage any discussion of digital risks.
- Children rely primarily on peers for advice instead of adults.

Teachers also rely heavily on manual systems—verbal reporting, logbooks, diaries—with no standardized follow-up procedures.

Parents expressed strong advocacy for integrating online safety into the curriculum, noting, "The Ministry of Education should make internet safety education mandatory, even in rural schools" (KII_PAR_1).

The validation workshop deepened this insight. Participants stressed that:

- A "social culture of silence" exists around digital harm.
- Teachers often have limited digital skills themselves.
- School leadership rarely discusses online child safety during assemblies or PTA meetings.
- Reporting in schools is not yet "normalized."

Victim-blaming attitudes remain pervasive. NGO respondents recounted instances where teachers chastised children for sending images instead of offering help (KII_NGO_3). Such responses reinforce shame and silence.

5.1.4 Police and Legal Pathways

Mistrust of police is a central social barrier. Children and caregivers view police stations as intimidating, insensitive, or unsafe. NGO respondents shared cases where officers minimized violations: "You tell the police the girl is 14, and they reply, 'but she already looks grown'" (KII_NGO_1).

Children in FGDs described their experiences with police as discouraging:

- "They ask too many questions."
- "They laugh."
- "They don't believe us."

Parents feared community stigma. Reporting to chiefs or police risks information leaks: "Soon everyone knows your business" (KII_INST_1).

The validation workshop emphasized how victim-blaming and cultural norms (especially those regarding sexual exploitation) discourage children from seeking help. This aligns with regional findings: ECPAT's research shows that across Africa, norms of silence and shame frequently prevent victims from reporting.

5.1.5 Community and Informal Mechanisms

Community-level barriers are shaped by cultural taboos around sexuality, fear of shame, normalization of silence, and reliance on informal settlement. An institutional respondent said, "People don't report because they think they are protecting their child's reputation" (KII_INST_1).

NGO respondents added that cases often "end up localized," with chiefs or elders handling matters quietly and no justice delivered (KII_NGO_1).

The workshop discussion highlighted that many communities encourage coping strategies (such as deleting messages, blocking perpetrators, or ignoring harassment) preferable to formal reporting.

Yet, community structures hold promise. Faith-based organizations were cited as important facilitators of online safety education. "Organizations like Compassion International and Watoto Watch teach parents and children through church networks" (KII_INST_1). Such trusted community intermediaries could help shift harmful norms if supported with training and clear reporting pathways.

5.2 Structural Challenges

Structural barriers relate to weaknesses in policy design and enforcement, institutional coordination, and resource allocation across the child protection ecosystem. Stakeholders in the validation workshop repeatedly stressed that, even where Kenya has made progress in law and policy, "the way the system is organized" often prevents existing mechanisms from working together effectively. These weaknesses are evident across online platforms, schools, police and legal pathways, and community-level structures.

5.2.1 Online Platforms

At institutional level, coordination between government agencies and digital platforms is fragmented and opaque. A national NGO leader observed that "there's no clear joint protocol between DCI, CAK, and platforms like Meta or TikTok on child exploitation cases" (KII_NGO_6). While the Communications Authority of Kenya (CAK) is mandated to regulate platforms and has signed agreements with tech companies, operational linkages with investigative bodies are weak.

Workshop participants explained that, in practice, the DCI Child Protection Unit must go through CAK to request preservation or release of digital evidence, rather than communicating directly with platforms. This creates delays and uncertainty for both investigators and survivors. Even civil-society actors face confusion when making referrals: "We receive a case and we are not sure—do we send it to CA, to DCI, or to the helpline? Often the same case is reported twice, and no one is sure who is following up."

Stakeholders also highlighted that tech companies have developed their own safety policies, but implementation and user awareness are uneven. "TikTok is trying, Meta has guidelines, but awareness among parents is very low," reported one NGO respondent (KII_NGO_1). Different platforms offer different reporting processes and categories, which users must learn separately. Participants described this as "mentally exhausting" for both adults and children. The validation meeting emphasized the need for more harmonized, user-friendly guidance on how to report, regardless of platform.

Data fragmentation was identified as a major structural gap. CAK, DCI, Childline Kenya, and other agencies all collect data using separate systems and policies, with no unified reporting database. Civil-society organizations expressed frustration that they "cannot tell if cases are being handled" because each institution "has its own data and cannot easily feed into CPIMS or a common dashboard." This institutional isolation undermines accountability, complicates follow-up with survivors, and limits Kenya's ability to build a comprehensive picture of online child abuse trends.

5.2.2 School-Based Reporting

Schools are a critical structural node, but they currently operate without standardized safeguarding frameworks for online child protection. KIIs and FGDs confirmed that "schools are the most consistent touchpoint for children, but there are no clear mechanisms for digital abuse reporting" (KII_NGO_4 & KII_NGO_5).

Teachers typically rely on informal hierarchies: a child tells a trusted teacher, who may inform the deputy or head teacher verbally. In FGD_INST_1, educators from "Code with Kids" described how they had developed internal escalation procedures within their institution, but acknowledged that "outside private institutions, there is no such structure."

The validation workshop deepened this picture. Stakeholders noted that schools receive mixed signals about their role in digital safety. On one hand, national policies discourage learners from bringing phones to school, leading some teachers to treat online abuse as "a home issue" and

refuse to intervene even when cyberbullying occurs between classmates. On the other hand, earlier government programs introduced digital devices into classrooms, creating expectations of early digital engagement without embedding corresponding safeguarding guidance.

Participants agreed that this ambiguity leaves individual teachers to decide what to do, often based on personal beliefs rather than formal policy. Some prioritize keeping children away from online spaces altogether; others allow ad hoc access without clear rules. One stakeholder emphasized that schools lack any specific guideline on handling online cases: "For physical abuse, they know where to escalate. For online, we have nothing."

Parents and NGOs proposed that every school should have a designated safeguarding lead and written procedures for online child protection, endorsed by the Ministry of Education and linked to the Directorate of Children Services. Without such frameworks, schools cannot reliably function as reporting or referral hubs, despite being where children spend most of their time.

5.2.3 Police and Legal Pathways

Participants acknowledged that Kenya has made important legislative advances (incluing the Children Act (2022), the Data Protection Act, and the Computer Misuse and Cybercrimes Act) but implementation remains inconsistent. One NGO respondent remarked, "We have good laws, but many officers still refer to the old Children's Act" (KII_NGO_2). Another noted that police often misclassify online offences: "They record grooming or image-based abuse as truancy or neglect because they don't understand cybercrime" (KII_NGO_6).

The validation workshop added further nuance on institutional capacity. Law-enforcement desks that handle child and domestic issues are often staffed by officers who are perceived internally as lower-priority or underperforming, suggesting that online child safety is not yet treated as a core policing function. One stakeholder observed that reporting desks can be seen as "places where officers who didn't perform well in other units are posted," which undermines both competence and public confidence.

High staff turnover compounds this problem. NGOs reported that they invest in training officers on child online protection, only for those officers to be transferred within months (KII_NGO_2). Participants suggested that police academies, such as Kiganjo, should integrate online child protection into their core curriculum, rather than relying on ad hoc in-service training.

Workshop discussions also emphasized a lack of practical tools and precedents. Stakeholders highlighted the need for clear charge sheets and case examples for online offences so that officers can understand how to frame charges and gather evidence. Without this, even strong laws remain underused.

Parents' testimonies illustrated the impact of these structural weaknesses: "You report, they take statements, and nothing happens" (KII_PAR_1). This contributes to a pervasive perception that online child protection cases are "not serious" or "domestic issues" that can be sidelined. Such institutional attitudes reinforce the trust deficit already documented in the social domain and discourage survivors from engaging formal legal pathways.

5.2.4 Community and Informal Mechanisms

At community level, child protection structures are heavily relied upon but poorly linked to national systems and chronically under-resourced. Chiefs and assistant chiefs were consistently identified

as first responders when children or families seek help. NGO respondents noted that "chiefs' offices are the first point of contact but they don't have digital reporting tools" (KII_NGO_3).

The validation workshop, however, highlighted a more complex picture. While earlier studies and regional data suggest that chiefs and community leaders handle a large share of cases, participants pointed out that attendance at chief's barazas is declining in more urbanized areas; some forums attract fewer than ten people. This raises questions about the continued effectiveness of traditional public forums as primary awareness and reporting channels, especially for adolescents who may not attend barazas at all.

Despite these shifts, community systems remain central for many families, particularly in informal settlements and rural areas. Participants cited evidence from regional access-to-justice studies showing that community structures are often perceived as more accessible, faster, and less intimidating than formal courts or police. In practice, however, chiefs and village elders rarely have formal guidance on handling online cases, and their decisions may not be documented or escalated.

Budget constraints significantly limit community-level action. One NGO respondent noted that "only about 150 shillings per child is allocated for protection annually—that's negligible" (KII_NGO_4). Workshop participants suggested that mechanisms such as the Child Welfare Fund could be leveraged in future to support community-based awareness and reporting efforts, including the provision of simple digital tools and training for chiefs and community volunteers.

Civil-society and faith-based organizations fill important gaps by offering awareness sessions, psychosocial support, and informal referral pathways. Yet these actors operate largely in silos, without systematic inclusion in national coordination forums. The validation meeting highlighted potential entry points for better coordination, such as Area Advisory Councils, Court Users Committees, and county-level child protection forums. Participants argued that online child safety stakeholders need to be "more visible and consistent" within these existing structures so that online reporting can be integrated into broader child protection planning.

5.3 Technological Challenges

Technological barriers relate to infrastructure, usability, data systems, and the digital divide. All of these shape whether existing reporting mechanisms feel accessible, safe, and worth using. Across the pathways, respondents repeatedly linked technology with two core concerns: lack of anonymity and weak interoperability between systems.

5.3.1 Online Platforms

On online platforms, accessibility, anonymity, and language limitations emerged as the main technological deterrents. Respondents expressed concern that platform-based reporting tools are tied to personal accounts and devices: "You report using your profile, so they can see you" (KII_NGO_3). Children echoed this anxiety: "If I report with my phone, they'll find out" (FGD_CHD_2). For many users, the fact that reporting requires being logged in, or using a personal smartphone, automatically undermines trust in the promise of confidentiality.

Participants also highlighted limitations in current content moderation systems. As one NGO respondent explained, "Someone can post abusive language in Kikamba or Dholuo and the platform won't detect it" (KII_NGO_1). Validation workshop discussions underscored that most moderation relies on machine learning trained in dominant global languages and supported by human moderators based outside Kenya, who "do not know Swahili or local languages." This creates a situation where grooming, bullying, or sexualized content in vernacular may bypass automated filters or be dismissed at review stage – even when local users recognize it as harmful.

A stakeholder noted that improving this situation requires deliberate collaboration between tech companies and local experts to "feed the machines" with accurate linguistic data from Kenyan and other African languages, yet this is only beginning to be explored and will take time to operationalize.

Usability Walkthroughs with children and adults further revealed that platform design often does not match the way young users navigate digital spaces. Participants struggled to locate safety sections or reporting icons on platforms such as TikTok, Instagram, and Facebook. Once found, reporting flows were described as "too long," "too many options," and "full of English text" that felt intimidating. Children showed a clear preference for:

- simple, visually prominent "click-to-report" icons
- minimal steps in the reporting journey
- the option to describe their experience in their own words, rather than selecting from rigid predefined categories

As one stakeholder observed, many young people "would rather just write out exactly what it is they were facing" instead of ticking unfamiliar labels. The combination of complex menus, and language constraints means that, even where platform tools exist, they are not designed in a child-centered way that supports real-world usage in Kenya.

KII_NGO_6 and others suggested that Kenya may also benefit from "homegrown platforms with data hosted locally," which could be better aligned with local languages, legal standards, and expectations of data sovereignty. However, such proposals will only be viable if they can match the usability standards children already experience on global platforms.

5.3.2 Helplines and SMS Services

Technological and logistical issues significantly limit the effectiveness of helplines as digital reporting tools. Participants reported "poor call quality, line congestion, and long queues" when attempting to contact 116 (KII_NGO_2; FGD_PAR_1). Children recounted instances where "the number doesn't go through" or "it takes too long to respond" (FGD_CHD_1). Usability testing during the study confirmed inconsistent response times as some calls were answered within a few seconds, while others took much longer, reinforcing the perception that the system is unreliable.

Parents expressed frustration not only with reaching the helpline but also with the absence of feedback: "You report and nobody calls back" (KII_PAR_2). From a technological perspective, this is closely linked to weak integration between helpline case-management systems and other national databases.

In the validation workshop, one stakeholder explained that CPIMS (Child Protection Information Management System) is currently linked to the child helpline and to tools such as Vurugu Mapper, yet this integration remains partial. Data from other actors like DCI's Anti-Human Trafficking and Child Protection Unit are not systematically fed into CPIMS, nor is there routine cross-sharing with education systems like NEMIS (National Education Management Information System). This limits real-time updates and makes it difficult to provide reporters with progress information.

Stakeholders recommended:

- stronger API-based linkages between CPIMS, helpline systems, DCI databases, and tools such as Vurugu Mapper and the Child Justice Information Management System
- simple, memorable USSD codes for reporting that work on basic phones without data (KII_INST_1)
- automated feedback mechanisms (e.g., SMS status updates) so that parents and children know their reports are being acted on

Without these improvements, helplines risk remaining "black boxes" where information enters but rarely returns to the child, caregiver, or frontline worker.

5.3.3 School-Based Reporting

Technological barriers in schools are stark and closely tied to broader inequalities in infrastructure. Most public schools lack reliable internet access, computers, or digital child protection databases. Teachers therefore rely on paper-based logs, punishment books, and personal diaries. As one educator explained, "We still use the punishment book or record in our diary" (FGD_INST_1).

In rural areas, children reported having to "borrow teachers' phones to access the internet" (FGD_CHD_1). This arrangement raises multiple concerns: limited privacy for the child, blurred boundaries around evidence collection, and the risk that images or messages captured as proof may be stored on a teacher's personal device without clear safeguards. One stakeholder noted that such practices can "compromise the quality of evidence" if cases later move into formal investigation.

The digital divide between well-resourced and under-resourced schools was repeatedly emphasized. "Informed schools with private sponsors can integrate ICT for reporting, but rural schools are in the dark" (KII_NGO_4 & KII_NGO_5). While institutions such as "Code with Kids" have internal reporting procedures and digital escalation protocols (FGD_INST_1), these are exceptions rather than the norm.

Respondents suggested that expanding Universal Service Fund (USF) investments to cover school connectivity would significantly strengthen both preventive education and reporting. However, connectivity alone is insufficient: schools also need simple digital tools (e.g., secure online forms or tablets linked to CPIMS), clear guidance on how to document online cases, and training on how to store and transmit digital evidence safely.

5.3.4 Police and Legal Pathways

Within law enforcement, technological capacity is a critical bottleneck. NGO and institutional respondents noted that many police stations lack basic internet access, dedicated computers, secure email, or specialized tools for handling digital evidence (KII_INST_1; KII_NGO_6). Officers therefore rely on manual registers and paper files, which increases the risk of delays, misplacement of records, and difficulty in tracking case outcomes.

One NGO representative summarized the interoperability challenge: "There's no interoperability between DCI cyber units and county police" (KII_NGO_1). The DCI cybercrime and AHTCPU units were widely praised for their technical competence but described as "very limited" in reach, with most child protection desks at station level lacking the capacity to identify, preserve, and forward digital evidence consistently.

The absence of secure, standardized communication channels between CPIMS, police systems, and prosecutorial databases also prevents effective feedback loops. As a stakeholder noted, because CPIMS is not linked to the systems used by investigators, children's officers "are not able

to get feedback, not unless you ask for it," which in turn prevents them from updating survivors and their families.

Respondents advocated for:

- phased digitization of police reporting and case-management systems, with child protection modules
- secure, role-based access that protects survivor data while enabling necessary coordination
- integration with CPIMS and other justice-sector platforms (such as the Child Justice Information Management System) to allow real-time status tracking of cases

Without these investments, even the best legal frameworks will continue to be implemented through analog processes that cannot keep pace with the speed and complexity of online offences.

5.3.5 Community and Informal Mechanisms

At community level, technological barriers are closely tied to poverty, geography, and the structure of local justice systems. FGDs with parents revealed a heavy reliance on face-to-face reporting: "We don't use the internet; we walk to the chief's office and explain" (FGD_PAR_2). For many households, low smartphone ownership, high data costs, and limited digital literacy make online reporting unrealistic (Etyang, 2025, p. 26).

At the same time, chiefs and community leaders increasingly have access to digital tools, but these are unevenly deployed. Past initiatives which include the Child Justice Information Management System have piloted providing chiefs with tablets or digital interfaces to record cases, yet these remain fragmented, and not all chiefs have been trained or equipped. A stakeholder noted that "the chief may be the only person with the technology or the capacity," which means that communities depend on him or her not just socially but technologically.

Participants highlighted the growing use of USSD-based tools and simple mobile applications as promising bridges for communities without reliable internet. Such approaches could allow parents or paralegals to file basic reports using feature phones, with chiefs or children's officers completing more detailed entries into national systems later.

Despite the constraints, there are encouraging examples. "Compassion International trains parents and children on data safety through community centers," reported one institutional actor (KII_INST_1), illustrating how digital literacy and protection skills can be delivered in places where online access is limited. Respondents stressed that when community training programmes are combined with investments in basic infrastructure (for example, shared devices at community centers, secure data connections for chiefs, and standardized tools linked to CPIMS), they can gradually narrow the technological gap.

5.4 Cross-Domain Synthesis

Across domains, the findings reveal a reinforcing cycle of mistrust, fragmentation, and exclusion.

- Socially, awareness and stigma dominate, deterring children and caregivers from seeking help.
- Structurally, institutions lack coordinated systems, clear mandates, and adequate funding.
- Technologically, inequities in access, design, and interoperability undermine the potential of digital reporting mechanisms.

Respondents repeatedly emphasized that effective reporting is not only about creating mechanisms but ensuring those mechanisms are trusted, understood, and responsive. Children need assurance of confidentiality; parents require literacy and confidence; and institutions need functional coordination across government, civil society, and technology actors.

Unless mistrust, fragmentation, and exclusion are addressed simultaneously across the social, structural, and technological domains, Kenya's expanding digital infrastructure will continue to outpace its capacity to protect children and respond effectively when harm occurs.

5.5 Conclusion

The study shows that barriers to effective reporting of online child safety issues in Kenya are deeply interconnected across social, structural, and technological domains. Socially, children and caregivers operate within a context of stigma, fear of exposure, and limited guidance on "what to do next" after harm occurs. Structurally, fragmented mandates, weak coordination between agencies, and under-resourced institutions mean that even when cases are reported, responses are slow, inconsistent, or invisible to survivors. Technologically, gaps in infrastructure, child-unfriendly design, and limited interoperability across systems restrict both access and trust in existing mechanisms.

Stakeholders in the validation workshop were clear that while awareness and technology matter, lasting change will depend first on structural reforms. If institutions cannot follow through on reported matters, new apps or campaigns will have limited impact. Strengthening the capacity of police, children's officers, helplines, schools, and courts to receive, document, investigate, and conclude online cases is therefore an urgent priority. Participants emphasized the need for clear protocols shared across platforms and agencies, better linkage of systems through CPIMS and related tools, and deliberate use of precedent cases (including strategic public interest litigation) to demonstrate that perpetrators of online abuse can and do face consequences. Visible prosecutions and coherent case-tracking would signal to children and caregivers that "reporting leads somewhere," helping to rebuild trust.

The findings also point to concrete, practical entry points for collaborative action. These include developing national guidelines for schools on handling online incidents and equipping them with basic digital reporting tools; engaging court stations and Court Users Committees to adopt simple, standardized charts and procedures for online child protection cases; and exploring stronger partnerships between government and tech companies so that reports made on platforms can trigger timely, coordinated action by law-enforcement agencies. At community level, investing in chiefs, paralegals, faith-based organizations, and other first responders, while also re-examining where children and adolescents actually turn first, can help anchor digital mechanisms within trusted local relationships.

Ultimately, safeguarding Kenya's children online requires moving beyond isolated awareness drives or stand-alone technological fixes. It calls for a coordinated, well-resourced ecosystem in which social norms support disclosure, institutions are capable and accountable, and technologies are designed around children's realities that are simple, safe, and responsive. If structural capacity is strengthened, platforms are made easier and more uniform to use, and survivors consistently see that reporting leads to protection and justice, then children will be far more likely to speak up. Only in such an environment can every child's voice count – safely, confidently, and effectively – within Kenya's rapidly expanding digital space.

5.6 Recommendations

The study outlines a range of practical suggestions in the social, structural, and technological spheres that can strengthen the online child-safety reporting system in Kenya. The research outlines a range of practical suggestions in the social, structural, and technological spheres that can strengthen the online child-safety reporting system in Kenya. These recommendations call for a more collaborative, people-centered approach that blends community trust, institutional strength, and practical technology. The study's evidence points to a clear path forward, built on making reporting easier, safer, and more meaningful for children and the adults who support them.

Strengthening awareness and digital literacy is an essential starting point. Children, parents, and teachers need simple, relatable guidance on what online harm looks like and what to do when it happens. Embedding this knowledge in schools through the curriculum and through co-curricular activities helps normalize conversations that many families still find difficult. Communities also have an important role: churches, chiefs, and grassroots organizations can create safe spaces where stigma is challenged and disclosure becomes more acceptable. When awareness campaigns are rooted in local languages and everyday experiences, they become far more effective.

Institutional capacity must evolve in tandem. Reporting is only useful if systems respond quickly and consistently, and that requires stronger coordination across agencies. Linking helplines, police units, schools, and social services through the Child Protection Information Management System (CPIMS) can help eliminate the silos that currently slow progress. Clear protocols should guide how cases move from one actor to the next, reducing the uncertainty that often frustrates reporting. Sustainable funding is equally important, as overstretched teams cannot deliver the timely support children deserve. Building online child protection modules into teacher training, police academies, and children's officer programmes ensures that frontline workers are prepared for the digital realities they encounter daily.

Technological improvements should focus less on novelty and more on usability and trust. Children repeatedly highlighted the need for reporting tools that feel intuitive, anonymous, and safe. Designing interfaces that require minimal information, work smoothly on basic devices, and are available in local languages would remove many of today's barriers. For communities with limited connectivity, USSD short-codes, zero-rated platforms, and shared devices in schools or community centers can expand access. At the same time, digital systems across government need to "talk to each other" so that reports are not trapped in isolated databases. Interoperability with social media platforms as well as national agencies would also make responses faster and more coordinated.

Community-level actors remain vital. Chiefs, assistant chiefs, and faith-based leaders are often the first people families turn to, yet they lack standard tools or guidance. Providing them with simple digital reporting aids and clear referral steps would help bridge the gap between informal disclosure and formal action. When these local structures are woven into county child protection forums and Court Users Committees, they can feed into the national system more effectively.

Across all these areas, collaboration is key. Government agencies, tech companies, and civil-society organizations must work more closely to align platform-level reporting with national procedures. Regular joint reviews of data that is reported, how cases progress, and where bottlenecks emerge, would make the entire ecosystem more transparent and accountable. Above all, reporting pathways must give survivors timely feedback. When children and caregivers see that reports lead to real action, trust grows, and reporting becomes a natural response rather than a last resort.

Taken together, these recommendations offer a pathway toward a more responsive, inclusive, and child-centered reporting ecosystem that is capable of keeping pace with Kenya's rapidly evolving digital world.

6. Annexes

- Matrix of Barriers and Opportunities Across Reporting Pathways.

DORMAIN	REPORTING PATHWAY	KEY BARRIERS IDENTIFIED	OPPORTUNITIES/ RECOMMENDATIONS
Social Challenges	Online Platforms	Low awareness of reporting tools; Fear of exposure; Distrust in systems; Cultural stigma.	Digital literacy campaigns for parents & children; Anonymous reporting; Local-language guidance.
	Helplines & SMS Services	Limited awareness; Caller traceability; Delays; Fear of judgment.	Rebrand 116; Real-time feedback; Anonymity protocols; Counseling follow-up units.
	School-Based Reporting	Untrained teachers; Fear of blame; Manual logs; Lack of frameworks.	Train teachers; Integrate safety into curriculum; Develop reporting templates linked to DCS.
	Police & Legal Pathways	Mistrust of police; Victim-blaming; Breach of confidentiality.	Train officers; Build trust; Child-friendly procedures; Anonymous reporting.
	Community & Informal Mechanisms	Cultural silence; Informal settlements; Weak linkages; Low awareness.	Engage faith & community leaders; MOUs for referral; Community champions.
Structural Challenges	Online Platforms	Weak coordination; Poor enforcement; No joint protocols.	Formalize CAK-DCI-platform MOUs; Taskforce; Enforce Data Protection Act.
	Helplines & SMS Services	Isolation of services; Underfunding; No case tracking.	Integrate into CPIMS; SOPs; Increase funding; Data sharing agreements.
	School-Based Reporting	No safeguarding frameworks; Weak referrals; Inequality between schools.	Safeguarding policy; Train focal teachers; County-level safe school networks.
	Police & Legal Pathways	Knowledge gaps; Poor tools; Frequent transfers; Corruption.	Police academy training; Forensic tools; Case digitization; Monitoring.
Technological Challenges	Community & Informal Mechanisms	Untrained chiefs; Poor documentation; Low budget.	Train local leaders; Referral cards; Include in county protection plans.
	Online Platforms	Lack of anonymity; Language barriers; Weak UX; Privacy risks.	Localized AI moderation; Encryption; Child-friendly design.
	Helplines & SMS Services	Network congestion; Long hotline numbers; No integration.	Short universal code; Two-way SMS; Link helplines to CPIMS.
	LSchool-Based Reporting	ow connectivity; Manual records; No ICT tools.	Expand school internet via USF; Digital dashboards; ICT clubs training.

	Police & Legal Pathways	Paper-based systems; No digital linkage; Limited tech tools.	Digitize records; Mobile data collection; Secure agency systems.
	Community & Informal Mechanisms	Low smartphone use; High data costs; Poor digital literacy.	Zero-rated apps; Community internet hubs; Literacy training.

6.2 References

African Union. (2020). Digital transformation strategy for Africa (2020–2030). African Union Commission.

Bronfenbrenner, U. (1979). The ecology of human development: Experiments by nature and design. Harvard University Press.

ChildFund & African Child Policy Forum. (2024). Online sexual exploitation and abuse of children: Scale, drivers, and impact in Africa. ChildFund Kenya.

CIPESA. (2025). Child protection and safety online in Africa: Regional status report. Collaboration on International ICT Policy for East and Southern Africa.

Communications Authority of Kenya. (2025). Quarterly sector statistics report, Q3 FY 2024/25. CA Kenya.

DataReportal. (2024). Digital 2024: Kenya. https://datareportal.com/reports/digital-2024-kenya

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.

ECPAT International. (2018). Trends in online child sexual abuse material: An exploratory analysis. ECPAT International.

ECPAT International, INTERPOL, & UNICEF. (2021). Disrupting harm in Kenya: Evidence on online child sexual exploitation and abuse. UNICEF.

Etyang, L. (2025). Exploring the link between digital literacy and safety among Kenyan children. African Institute for Children Studies.

Global Partnership to End Violence Against Children. (2023). Tackling online violence against children: Global review and recommendations. End Violence Lab.

Internews. (2024). Digital information ecosystem assessment: Understanding Kenya's online environment and emerging risks. Internews Network.

International Telecommunication Union. (2023). Child online protection guidelines. ITU Publications.

KICTANet, BAKE, Internews, Internet Without Borders, Tribeless Youth, Mzalendo Trust, & Watoto Watch Network. (2025). KenSafeSpace programme framework. Kenya Safe and Inclusive Digital Space Consortium.

National Council for Children's Services. (2022). National plan of action to tackle online child sexual exploitation and abuse in Kenya (2022–2026). NCCS.

Ndemo, B., & Munyuwiny, S. (2018). Baseline study on child online safety in Kenya. Terre des Hommes Netherlands.

Ochieng, M. A. (2023). Factors influencing children's vulnerability to online child sexual exploitation in Kenya (Master's thesis, University of Nairobi).

OECD. (2020). Protecting children online: Risks, harm and policies across countries. OECD Publishing.

UNICEF. (2021). Global strategy for online child safety. UNICEF.

World Health Organization. (2020). INSPIRE: Seven strategies for ending violence against children. WHO Press.

Watoto Watch Network

CONTACTS

Tel: +254 743 379 789
Web: https://watotowatchnetwork.org/
WATOTO WATCH NEWORK