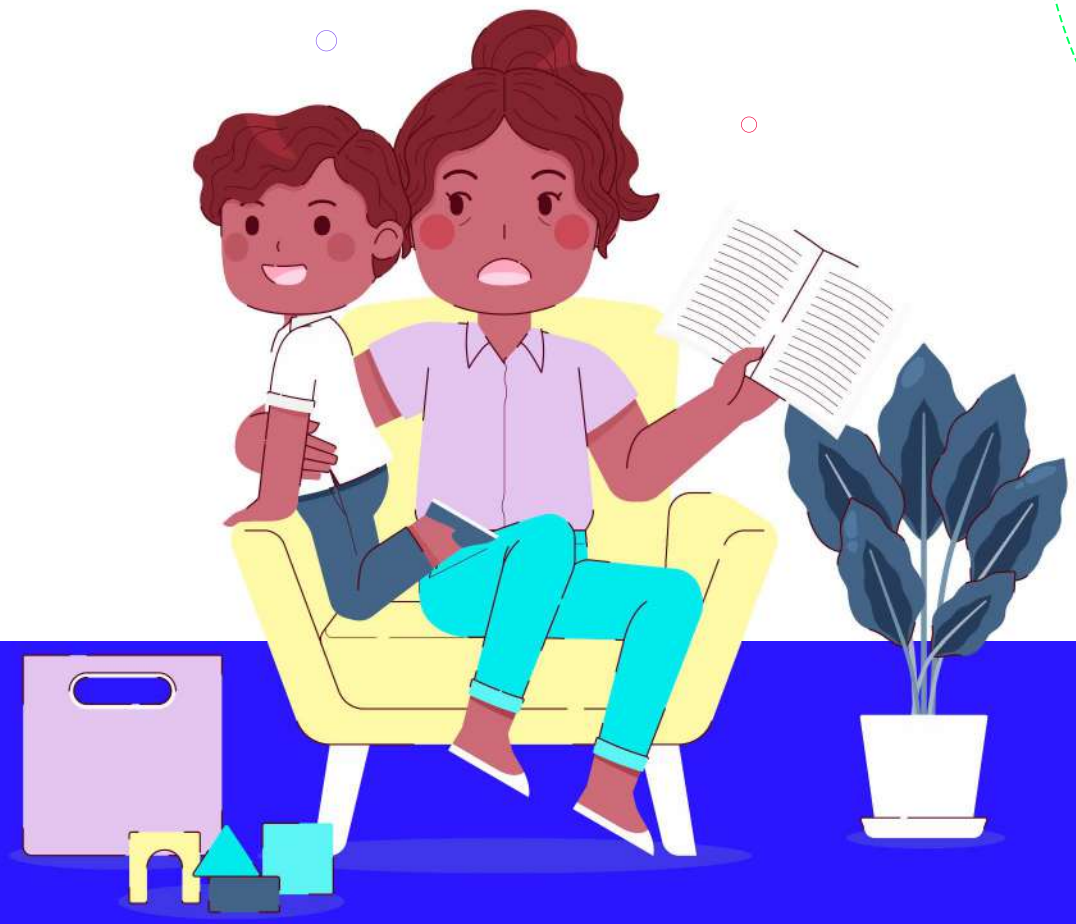
TECH HIVE
ADVISORY

A Guide To Raising Safe Kids Online



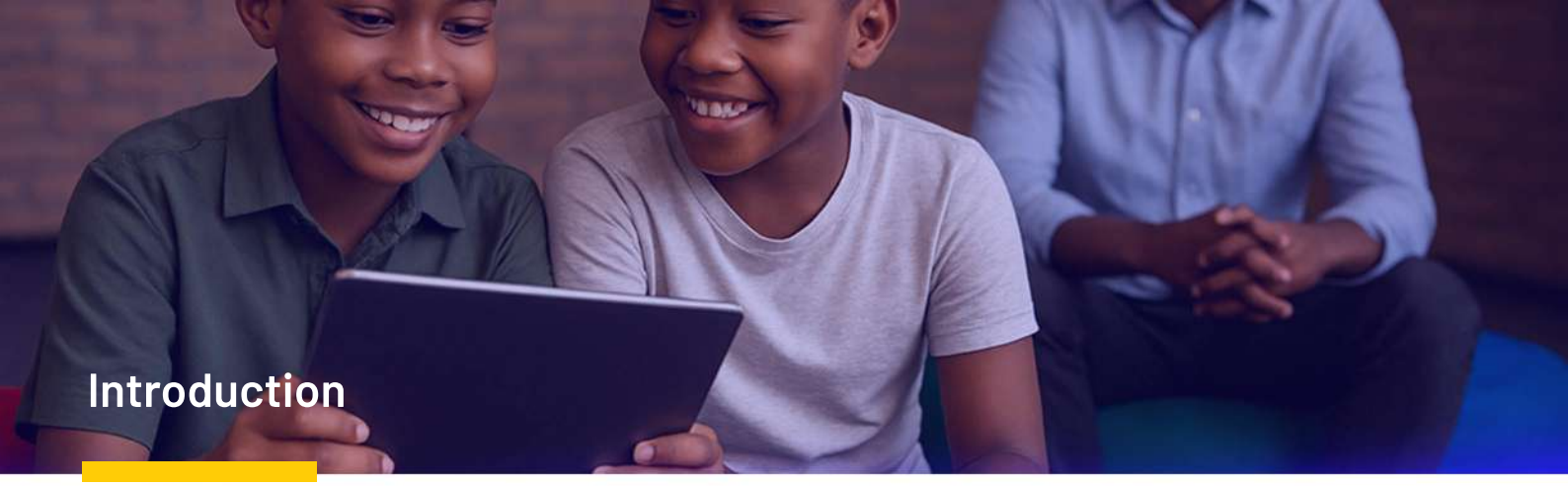
List of contributors:

1. Ridwan Oloyede
2. Wisdom Agbonyehemen
3. Lauretta Onwuegbuzie
4. Rodiyyah Bashir
5. Fopefoluwa Ibraheem

Designed by:

Adeyinka Adeyemo

Table of Contents



Introduction

The digital ecosystem has become the primary environment in which children learn, play, communicate, and grow. From online classrooms and gaming communities to social networks and AI-driven platforms, digital spaces now shape many aspects of childhood. This connectivity offers significant benefits, including enhanced learning opportunities, creative expression, social participation, and global friendships. However, it also poses risks such as cyberbullying, grooming, exposure to harmful content, misinformation, unfair algorithmic influences, privacy breaches, and exploitation. With the physical and digital worlds increasingly intertwined, protecting children online is not merely a matter of safety; it is a fundamental human rights obligation and a critical public policy priority in Africa and beyond.

This toolkit addresses children's online behaviours and trends, legal and policy frameworks, the roles of institutions and communities, safety measures, privacy protection, digital literacy, and the impacts of emerging technologies. It has been designed to remain relevant across diverse African contexts, reflecting local realities and values. It is intended to support policymakers, educators, parents, civil society organisations, and technology companies in understanding and responding to the challenges and opportunities of the digital world for children. ***The toolkit provides clear guidance, practical tools, and resources to safeguard children's rights, promote safety, and encourage positive digital experiences.***

Understanding The Digital Landscape For Kids

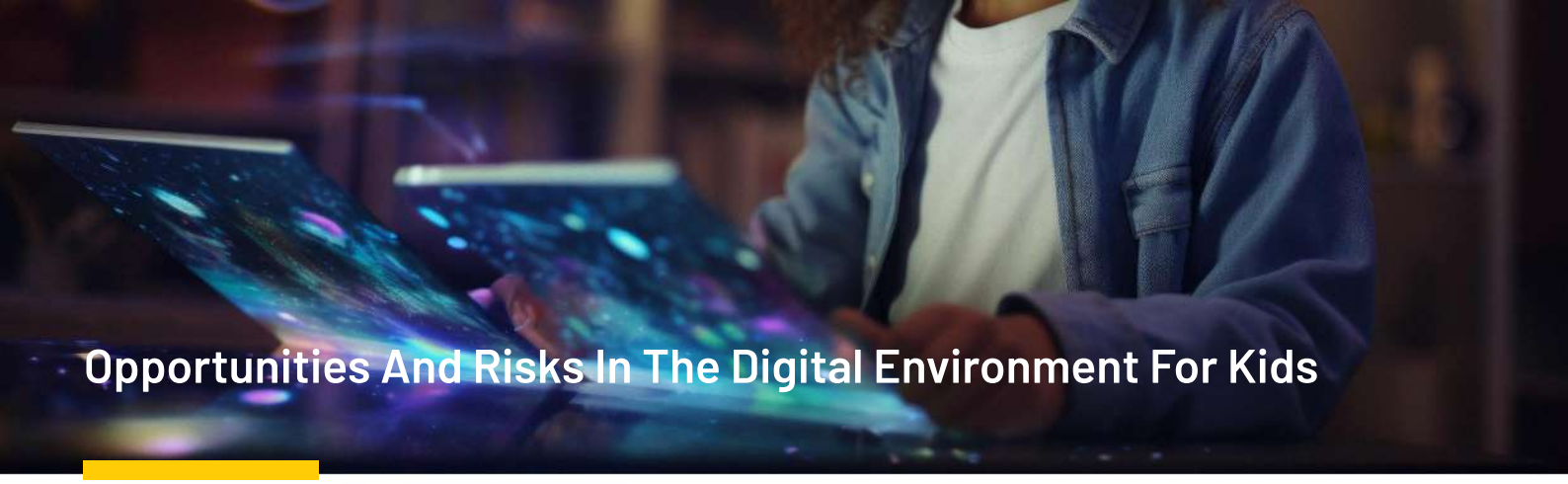
The digital world is an integral part of a child's life, shaping their social interactions, learning, and entertainment. A comprehensive online safety strategy must be built on a clear understanding of this ever-evolving environment, including how children engage with it, the inherent opportunities and risks, and the varying contexts in which they navigate it.

Children's Online Behaviours and Trends

Children's online activities are constantly changing and are currently driven by new technologies and social media platforms. They don't simply "use" the Internet; they live in a blended reality where online and offline experiences are deeply intertwined. ***Some of the interactions they have include:***

- **Social Interaction and Identity:** Social media platforms like TikTok, Instagram, and Snapchat are central to how children connect with peers, build communities, and express their identities. This often includes a heavy reliance on visual content, short-form video, and constant online communication. Research shows that girls tend to use social media more, while boys are more likely to engage in online gaming.[1]
- **Gaming and Entertainment:** Online gaming is a major activity, and it's no longer just a solo pursuit. Many games are social spaces where children communicate with friends and strangers. Platforms like YouTube and streaming services are also primary sources of entertainment and information, often surpassing traditional television.
- **Constant Connectivity:** A significant trend is the increasing amount of time children spend online. Nearly half of teens report being online almost constantly, and this "always-on" behaviour can have a direct impact on sleep, physical activity, and mental health.
- **Learning and Creativity:** The internet is a powerful tool for learning, allowing children to access information, develop new skills, and engage in creative activities like content creation, coding, and digital art.

[1]Spilková J, Chomynová P and Csémy L, 'Predictors of excessive use of social media and excessive online gaming in Czech teenagers' (2017) Journal of Behavioral Addictions 6(4) 611-619, doi:10.1556/2006.6.2017.064 ([pubmed.ncbi.nlm.nih.gov][1])



Opportunities And Risks In The Digital Environment For Kids

The online world presents a duality of experiences, offering immense benefits while also posing serious risks. It is crucial for caregivers and educators to understand both sides.

Opportunities:

- **Education and Skill Development:** Digital platforms provide access to a wealth of educational resources, from tutorials and online courses to collaborative learning tools, fostering self-directed learning and digital literacy.
- **Social Connection and Community:** For children, especially those who may feel isolated or marginalised, the internet offers a vital space to find and connect with like-minded individuals, build friendships, and find support networks.
- **Creativity and Self-Expression:** The digital environment empowers children to be creators, not just consumers. They can develop their talents through video production, music, writing, and art, sharing their work with a global audience.
- **Civic Engagement:** Digital tools can facilitate children's participation in social and political issues they care about, giving them a voice and a platform to advocate for change.

Risks:

- **Content Risks:** Exposure to harmful, inappropriate, or age-inappropriate content is a major concern. This includes violence, self-harm promotion, hate speech, and pornography, which can be encountered accidentally or through algorithms that push extreme content.
- **Contact Risks:** These are risks related to interactions with others. It includes cyberbullying from peers and more severe threats like grooming, where predators build trust with a child to facilitate sexual exploitation.
- **Conduct Risks:** Children can also be at risk due to their own behaviours. This can involve sharing too much personal information, participating in dangerous online challenges, or engaging in "sexting." The pressures of social media can lead to problematic use with symptoms similar to addiction, affecting mental well-being and social development.
- **Consumer Risks:** The digital environment can expose children to commercial risks, such as in-game purchases, targeted advertising, and scams. Design features like "loot boxes" and "time-limited offers" are often engineered to encourage impulsive spending.

African Child Online Safety Laws And Regulations

Across Africa, child online safety is gaining increasing legal recognition, with governments enacting laws and frameworks to safeguard children in the digital space. Many states are aligning with international conventions such as the UN Convention on the Rights of the Child and the African Charter on the Rights and Welfare of the Child, embedding principles of protection, safe access, and digital literacy. ***Key measures*** include provisions under data protection laws, cybercrime legislation, and emerging online safety policies, which collectively impose obligations on technology companies, internet service providers, and educational institutions. However, the landscape

Global Legal And Policy Frameworks

- **UN Convention on the Rights of the Child (UNCRC):** The UNCRC establishes children's civil, social and economic rights. States are required to protect children's privacy, dignity and protection from abuse, principles that extend into the digital sphere.

- **Optional Protocols to the UNCRC.** The Optional Protocol on the sale of children, child prostitution, and child pornography requires states to criminalise those offences and put protective measures in place. These protocols are the international legal backbone for prosecuting and preventing online sexual exploitation of children.

- **Regional instruments (Africa)** The African Union Convention on Cyber Security and Personal Data Protection; the "Malabo Convention" (adopted 2014) sets continent-level standards on cybersecurity, data protection, and e-commerce, and includes provisions relevant to child protection online. Note: the Convention requires ratification by member states to take full effect, and uptake has been slow in some regions.

- **Cybercrime frameworks:** The Council of Europe's Budapest Convention is widely used as a model for national cybercrime laws. It criminalises the production, possession, or distribution of child sexual abuse material (CSAM) and supports cross-border cooperation). Many countries look to it when drafting cybercrime legislation.

African Laws and Regulations

NIGERIA

- **Child's Rights Act (2003) –** The Act protects children's rights but is unevenly domesticated across states.

- **Cybercrimes Act (2015, amended 2024) –** This is the main law against online exploitation, grooming, and CSAM.

- **Nigeria Data Protection Act (2023) –** This Act regulates the processing of children's personal data and gives oversight powers to the data protection authority.

KENYA

- **Children Act (2022) –** This act aligns national law with the UNCRC; includes digital-age protections.
- **Data Protection Act (2019) –** This act introduces special categories for children's data and requires parental consent for under children under 18 years.
- **Computer Misuse and Cybercrimes Act (2018) –** This act criminalises child pornography and online abuse.

SOUTH AFRICA

- **Children's Act (2005) –** This act provides comprehensive protections against harms to children, this includes online exploitation.
- **Protection of Personal Information Act (POPIA, 2013) –** This act limits collection and use of children's personal data.
- **Films and Publications Amendment Act (2019) –** strengthens rules on distributing harmful digital content, especially CSAM.

GHANA

- **Children's Act (1998) –** This is the foundational law on child welfare, extended in practice to online contexts.
- **Cybersecurity Act (2020) –** This act establishes the Cybersecurity Authority and provides measures for child online protection.

Policy Gaps And Recommendations

Despite progress in child online safety regulation across Africa, significant policy gaps remain that limit the effectiveness of existing frameworks. These gaps arise from weak enforcement, fragmented policies, and limited awareness among stakeholders, leaving children vulnerable in the digital environment. Some of these gaps include fragmented legislation, weak enforcement mechanisms, limited awareness, and digital literacy.

Recommendations

- **Enhance Enforcement and Capacity Building :** Regulation without enforcement is ineffective. Dedicated units within regulators and law enforcement equipped with forensic AI tools, legal authority for data access, and training in child protection are essential to act swiftly against AI-driven harms such as online grooming or harmful algorithmic recommendations.Also, establishing hotlines and rapid response mechanisms ensures that harmful content is detected and removed within few hours.

- **Digital Literacy Programmmes:** Introduce nationwide digital literacy programmes in schools and community centres, co-designed with child psychologists and educators. Campaigns should target not only children but also parents and teachers, equipping them with tools to manage risks such as cyberbullying, grooming, and misinformation

- **Promote Regional Harmonisation and Cross-Border Cooperation:** The African Union (AU) should accelerate the development of a continental framework for child online safety, building on existing instruments such as the Malabo Convention on Cybersecurity and Data Protection. To complement this, regional blocs including ECOWAS, SADC, and EAC should establish cross-border reporting and enforcement mechanisms to address online child abuse cases effectively, ensuring consistency and cooperation across jurisdictions.

Why Is Multi-stakeholder Collaboration Essential In Enduring Online Safety For Kids?

Multi-stakeholder collaboration is very essential because no single actor can address the complexity of child online safety. Governments provide the legal framework, but platforms hold the tools to design safer systems, while NGOs, educators, helplines, and researchers contribute frontline expertise, advocacy, and evidence. Working together creates an ecosystem where responsibilities are shared, ensuring safeguards are holistic and responsive to emerging risks.

Equally important is grounding solutions in children's lived experiences. ***Involving their voices makes interventions more practical,*** while co-regulatory codes of conduct align industry innovation with public safety goals. Civil society and governments also strengthen awareness and digital literacy among parents and guardians, ensuring communities are empowered to protect children online.

Online Safety and Protection Measures For Kids

To safeguard children's well-being, it is essential to implement structured safety measures that empower children, guide parents and educators, and hold digital platforms accountable. These measures serve not only to protect children but also to create a safe, supportive, and enriching digital environment.

- **Secure Passwords:** Encourage the creation of strong, unique passwords combining letters, numbers, and symbols, avoiding easily guessable information.
- **Two-Factor Authentication (2FA):** Add an extra verification step when logging in to sensitive accounts, such as a code sent to a phone or email.

- ***Privacy Settings:*** Adjust privacy controls on social media platforms, apps, and online games to restrict who can see and interact with profiles.
- ***Content Filters and Parental Controls:*** Use software tools to block inappropriate content and tailor online access according to age-appropriate guidelines.
- ***Digital Literacy Education:*** Teach children how to identify fake news, scams, cyberbullying, and the importance of not sharing sensitive personal data.
- ***Device and App Monitoring:*** Utilize monitoring tools and set limits on screen time or usage schedules to balance online activities and offline life.
- ***Open Communication Channels:*** Encourage regular conversations about online experiences, challenges, and feelings without judgment or fear of punishment.
- ***Safe Social Networking Practices:*** Guide children on friend requests, commenting, sharing content, and reporting suspicious or harmful behaviour.
- ***Use of Secure Networks:*** Advocate connecting to trusted Wi-Fi networks, avoiding public unsecured connections that might expose data.
- ***Software and Device Updates:*** Keep operating systems and apps updated to protect against vulnerabilities and malware exposures.
- ***Reporting and Blocking Mechanisms:*** Teach children how to report inappropriate content or online abuse on platforms and block offenders promptly.
- ***Awareness of Digital Footprint;*** Make children aware that online actions leave a permanent trail that can affect their future reputation and privacy.

Implementing these measures *within communities, schools, and homes helps create a safer digital space tailored to the needs and vulnerabilities of children and young people, especially within diverse African contexts where digital access and literacy levels vary widely.*

Digital Literacy and Education

The reality is simple: children do not just "go online" anymore; they live online. From their classrooms to their playtime, and even in the friendships they form, digital spaces have become part of childhood itself. This change brings opportunities for growth and learning, but it also creates risks that earlier generations never had to navigate.

Digital literacy prepares them to stay safe, think critically, and make informed choices in the online world they are already immersed in. Without it, we leave them vulnerable. With it, we prepare them for both safety today and success tomorrow.

Curriculum Integration

Digital literacy should be embedded into the national curriculum framework as a recognised area of learning with clear objectives, age-appropriate milestones, and standards for assessment. This means children do not just "pick up" online safety lessons in passing. Instead, they progress through structured learning pathways, much like they do with mathematics or reading. In early years, they learn the basics of safe device use, asking for help, and understanding what is private.

In primary school, they move into critical thinking about online information, respectful online behaviour, and simple privacy settings. By secondary school, they are taught to evaluate complex digital content, recognise manipulation, understand digital rights, and protect their long-term digital footprint.

Curriculum integration ensures that digital safety is not left to chance or dependent on individual teachers' enthusiasm. It guarantees that every child, regardless of background, has access to the knowledge and skills needed to thrive safely in a digital-first world.

Teacher and Parent Training

Teachers and parents are the frontline guides for children in the digital space. But many adults feel overwhelmed by how fast technology changes. Training helps bridge this gap. For teachers, it means knowing how to spot when a child might be facing online harm, and feeling confident enough to teach new digital risks as they emerge.

For parents, it means learning practical steps; from using parental controls to having open conversations about what children see online. When schools and families are aligned, children get consistent guidance, both in class and at home.

Child Empowerment and Resilience

At the heart of digital literacy is empowerment. Children should not just be taught to avoid danger; they should grow confident and capable in their online lives. That means helping them to:

- Recognise risks and respond wisely.
- Control their privacy and security settings.
- Question the credibility of information, especially in a world of AI-driven content.
- Understand how their digital footprints shape their future opportunities.
- Build resilience, so that if they encounter harm, they know how to cope and seek help.

Empowered children are not passive users of technology. They are responsible digital citizens that can protect themselves, support their peers, and use online spaces for growth rather than harm.

Monitoring, Evaluation, And Assessment Of Children Online Safety

Key Performance Indicators (KPIs)

KPIs are measurable markers that show whether child online safety efforts are achieving results. For example:

- Number of schools that have integrated online safety into their curricula.
- Percentage of parents trained in digital literacy and parental control tools.
- Frequency of child-reported incidents of online harm (and response times).
- Reach and engagement of awareness campaigns (social media, webinars, workshops).
- Reduction in harmful exposure rates over time.

Well-chosen KPIs move the conversation from intentions to impact.

Feedback Loops and Continuous Improvement

The digital environment changes daily. Strategies that worked last year may not be enough tomorrow. This is why feedback loops are crucial.

- **Children's voices:** Regularly seeking feedback from children themselves about what risks they face and how safe they feel online.
- **Parent and teacher feedback:** Understanding the challenges they face in guiding or monitoring children's online behaviour.
- **Data-driven learning:** Using monitoring tools, reporting statistics, and surveys to refine policies and interventions.

Feedback loops ensure that programmes are not static but continuously adapted to meet real-world needs.

Conclusion

Child online safety is not a single policy issue it is a human rights imperative that cuts across education, technology, law, and community well-being. As children increasingly live, learn, and socialise in digital spaces, protecting them from exploitation, abuse, and harmful content must remain a collective responsibility.

This toolkit has outlined the global and regional frameworks, national laws, and practical protection measures that shape the digital environment for children. Yet, laws and policies alone are insufficient without enforcement, awareness, and active participation from all stakeholders. Governments must provide clear regulations and capacity; technology companies must design responsibly; educators and caregivers must foster digital literacy; and children themselves must be empowered to navigate online spaces safely.

Together, we can ensure that the internet remains not a place of fear, but a platform of empowerment for every child.