**Name (individual or organisation):** Collaboration on International ICT Policy for East and Southern Africa (CIPESA), International Center for Not-for-Profit Law (ICNL), and the Digital Rights Alliance Africa (DRAA)

**Category of stakeholder:** *Civil society*

**Country or countries your input primarily concerns***: East Africa (Kenya, Rwanda, and Uganda, Tanzania), North Africa (Algeria, Egypt), South Africa (South Africa, Botswana, Zimbabwe), and West Africa (Ghana, Nigeria)*

**Regions: *Africa*** *(East, North, South, and West)*

**Areas of Expertise or Focus:** Children's Online Protection and Safety, Digital Rights and Inclusion in Africa

## A) Risks to children's rights and safety in the digital environment

1. What are the most significant risks to children's safety, physical or mental health, and rights in the digital environment in your country or region, and how are they shaped by regional context?

*Consider: regional patterns and emerging threats; the drivers of risks to children's safety, physical and mental health and rights, including product design, business models, and connectivity and access gaps*.

The digital landscape in Africa has experienced a transformative shift, reshaping how children engage, learn, and exercise their rights both online and offline. This has brought with it numerous opportunities, as much as risks against children's online protection and safety.

The Digital Rights Alliance Africa's (DRAA) Report on *Child Protection and Safety Online in Africa* (hereby, DRAA, 2025) zooms in on the most pressing online harms posed against children in 10 African countries; Algeria, Botswana, Egypt, Ghana, Kenya, Nigeria, Rwanda, South Africa, Tanzania, and Uganda. Starting off with legal constraints, it highlights that most African countries treat privacy laws as general provisions, without considering the unique vulnerabilities faced by children in the digital environment. And even where laws exist, enforcement remains a major challenge. Additionally, while many African nations have signed international treaties such as the United Nations Convention on the Rights of the Child (UNCRC) and the African Charter on the Rights and Welfare of the Child (ACRWC), the domestication and enforcement of these standards

remains slow because of the dualist legal system in most member states. This has left children on the continent in a vulnerable state. Regulatory bodies tasked with protecting children's privacy online are often also under-resourced and lack the necessary capacity to monitor and enforce compliance.

Cyberbullying and harassment is a growing issue across Africa, fueled by increasing internet penetration and widespread use of social media platforms. And its proliferation is happening in the backdrop of the widespread use of social media that has created a sense of anonymity online. Children targeted by cyberbullying often face long-term emotional and psychological issues, including anxiety, depression, low self-esteem, and post-traumatic stress disorder (PTSD).The use of online platforms like Facebook and WhatsApp has overly exposed children to online grooming and exploitation due to minimal supervision in usage. Children have been exposed to sexual contact through online platforms leading to actual physical harm. Children's personal data privacy is breached and exploited by companies for commercial purposes, often without obtaining proper consent and failing to comply with local data protection regulations.

Emerging technologies such as Artificial Intelligence (AI) and their associated risks to children's online safety have also further exacerbated children's vulnerability including AI-generated sexual images and deepfakes, online impersonation, AI-enabled scams and financial exploitation through mobile money and digital platforms. According to the *INTERPOL member country survey in Africa of 2026,* Digital sextortion surged in 2025. Pertinent to children, UNICEF 2026 report titled 'Through Children's Eyes: How digital technologies enable child sexual abuse' shows the pervasiveness of AI-facilitated online harms posed against children in Africa. For instance, Uganda's survey data indicates that 38.5% of internet-using children aged 12-17 experienced at least one form of technology-facilitated sexual exploitation, for Kenya an average 26.8%, with about 1.3 million children affected while Tanzania was at 9.0%.

According to DRAA's Report (2025), the digital divide and lack of infrastructure in rural areas exacerbate privacy risks for children in Africa. The economic constraints in many African countries also mean that governments often lack the resources to implement comprehensive child protection policies. In some instances, economic constraints are compounded by political instability which further leads to the disruption of the development of cybersecurity infrastructure. Additionally, shortfalls in digital literacy in many African countries account for unintentional sharing of personal information, vulnerability to online risks such as phishing scams and general exposure to online digital security risks.

2. How do digital product design and business models drive or mitigate risks to children's rights online, including in AI-mediated products and services?

*Consider: algorithmic recommendations, notification systems, and engagement-optimized design; targeted advertising; data collection, profiling, and privacy; and generative AI.*

Global trends caution against the exposure and engagement of children to AI and AI-embedded platforms which have a risk of compromising their online protection and safety.

In tune with these trends from the African context, the lack of child-centric AI- strategies across Africa is risking AI technologies becoming tools of exploitation, as opposed to empowerment.

Children are increasingly exposed to wide-range of AI-driven harms and are disproportionately affected due to the digital divide, which undermines their awareness of these threats. This manifests in forms of exploitative data collection, algorithmic profiling, as well as exposure to biased, inappropriate content [CIPESA, *Elevating Children's Voices and Rights in AI Design and Online Spaces in Africa,* 2025; *State of Internet Freedom in Africa*, 2024].

Multi-stakeholder and collaborative initiatives like the Africa Taskforce on Child Online Protection composed of mobile industry, technology sector, regulatory bodies, law enforcement and civil society are emerging to coordinate responses to such risks and harms across the continent, while also offering a best practice which may be scaled and strengthened at the global level [UNICEF, *UNICEF and GSMA unite with partners to launch Africa Taskforce on Child Online Protection to safeguard children in the digital age,* 2025].

Such coordinated efforts are instrumental in facilitating the realisation of robust, well-coordinated, and practical steps to ensure rights-respecting business practices by addressing addictive design, and tightly regulating online marketing targeting children. These steps, in tune with the United Nations' (UN) Guiding Principles on Business and Human Rights, would also foresee the enforcement of due diligence centering children's rights, as well as establishment of transparency and accountability mechanisms to ensure effective redress for child survivors [CIPESA, *Protecting Children Online in Africa Must Move from Policy to Practice*, 2026; Office of the United Nations High Commissioner for Human Rights, *Getting Children's Safety Online Right*, 2026].

3. How are children's own views being sought and given due weight in the design, governance and regulation of digital environments in your region, by either companies or States?

*Consider: meaningful and safe participation of children, including those in vulnerable situations; how children's views are reflected in decisions, design and regulatory choices that affect them*.

The absence of children's voices and meaningful engagement in decision and policy-making processes remains a critical challenge in Africa and calls for more institutional strengthening on appropriate policy inclusion strategies. [CIPESA, *Elevating Children's Voices and Rights in AI Design and Online Spaces in Africa,* 2025]. Nevertheless, some efforts are worth considering.

At the continental level, children's engagement during the 48th ordinary session of the African Committee of experts on the Rights and Welfare of the Child (ACERWC) is exemplary in terms of shaping the agenda and advocating for themselves and their peers during high-level discussions including on the digital frontier and emerging risks and threats posted against them [ACERWC, *Day of General Discussion 2026, https://reporting.acerwc.africa/en/article/events/day-general-discussion-2026*]. IGAD's 2024 children's consultation on its Children Policy Framework is an equally noteworthy best practice for uptake in the area of digital rights [IGAD Hosts First-Ever Children Consultation Workshop on the IGAD Child Policy Framework, 2024].

Research consultations on children's experiences within the digital environment are notable [The London School of Economics and Political Science, *African children's rights in relation to the digital environment: child-informed provocations to guide digital policy and practice*, 2026]. There is also space for youth participation within the Africa Taskforce on Child Online Protection (COP)

which may be tailored and upscaled to meaningfully and safely engage children in topical discussions and decisions [UNICEF, *UNICEF and GSMA unite with partners to launch Africa Taskforce on Child Online Protection to safeguard children in the digital age,* 2025].

The above strategies highlight the need to fill in a critical gap in terms of the meaningful engagement of children (which goes beyond mere consultation), especially at the domestic level to enable them to participate in shaping policies and decisions that foster their digital safety across the continent. In this regard, AU's Guideline on Child Participation (2022) is instrumental 'to enhance the realisation of the right of children to participate and to be heard in all matters that affect them.'

4. How do digital environments, and the measures taken to make them safer, affect different groups of children differently — and how can equality and non-discrimination in access and protection be ensured?

*Consider: differential risks, protection and access (by age, gender, disability, minority or migration status, and socio-economic context); the digital divide; and whether protective or regulatory measures themselves produce discriminatory effects, e.g. excluding children without formal documentation.*

DRAA's Report (2025) findings underscore that an estimated 40% of African children aged 15 and above now have internet access, opening up new avenues for education and connectivity. And while digital literacy is essential for children to understand online risks and protect their privacy, many African countries face significant gaps in digital education. This lack of awareness leaves children vulnerable to online risks such as identity theft and exploitation, as they often do not understand the risks associated with sharing personal information online [DRAA, *Child Protection and Safety Online in Africa,* 2025].

The lack of infrastructure in rural areas further exacerbates privacy risks for children in Africa. Across the study countries, children in rural regions have little to no access to digital literacy programs or secure internet connections, making them more vulnerable to privacy violations. The regions are also characterised by limited access to technology and weak governance structures that make it difficult for the government to enforce privacy regulations effectively [DRAA, *Child Protection and Safety Online in Africa,* 2025].

These facts, together multiply the existing vulnerabilities of children in online spaces, by worsening the digital divide which pushes under and unrepresented communities in rural areas further to the margins of key dialogue and decision-making processes affecting their lives within/across online spaces.

Young girls are also increasingly becoming victims of Online Child Sexual Exploitation and Abuse (OCSEA) and technology-facilitated gender-based violence (TFGBV) across Africa. This is occurring in the backdrop of socio-cultural as well as legal and implementation barriers which hinder open dialogue, reporting, as well as effective and timely redress [ECPAT et al., *Girls & Young Women-Led Assessment on Online Sexual Exploitation, Abuse & Technology-Facilitated Gender-Based Violence in Africa*, 2025]. Children with disabilities are further disenfranchised by

systems which have been designed in lack of recognition of their unique needs and vulnerabilities as well.

In this regard, mitigating these challenges calls for policy and programmatic-level dialogue and decisions to ensure rights-respecting digital technologies and online spaces come to fruition. In turn, this would help shape policy priorities and investment decisions related to data generation, legal and institutional reform, digital and cybersecurity infrastructure, public awareness initiatives, and capacity building for key stakeholders, including judges, lawyers, advocates, and law enforcement officials. It would also promote multi-stakeholder dialogue and support meaningful community mobilization and engagement at both the national and sub-national levels.

Across all processes, children ought to be meaningfully engaged in cognizance of their interrelated rights, vulnerabilities and contexts, while ensuring the 'do no harm' principle.

5. How can children's digital literacy, skills and empowerment be supported, so that they can benefit from the opportunities of the digital environment and participate in it safely?

*Consider: digital literacy and competencies for children, parents, carers and educators; the role of schools and communities; and approaches that strengthen children's agency.*

Digital literacy initiatives may be supported by ensuring

- Their embedment within broader national development plans (in sync with regional and global-level commitments), which also promotes government-leadership, localization efforts, and the sustainability of interventions. Such approaches are also beneficial to address the protection needs of refugee and IDP children through an integrated education and digital literacy services tailored to their needs.
- Role sharing and commitments across the broader community engagement takes place, meaningfully.
- Participation in curricula design and development through integration of their voices, views, and lived experiences in specially tailored programs and policies. African children must be a part of the solution of their digital future.
- Programmatic synchronicity between interventions to ensure learning is duly documented, reported, and disseminated for policy uptake at the national, continental and global levels. Such practices will have significant value and contribution to the position of the continent and member states within global discourses on children's online protection and safety.
- Design and support systems which support disaggregated and analyzed data to inform how learning is translated into action plans for policy and decision-making at all levels.
- Design a universal and specialised education training on children's rights to protection and safety across online and offline spaces for learning programmes for children and parents, teachers, lawyers, civil society and other organisations.
- Adopt a robust stakeholder coordination across sectors and at all levels, which would also be instrumental to tackle siloed interventions, and duplications of efforts across member states.

**State obligations and regulatory responses**

6. What noteworthy legislative, policy and regulatory measures are being taken in your region to address risks to children's rights and well-being in the digital environment, and which are proving effective?

*Consider: legislative and regulatory frameworks addressing cybersecurity, harassment, child sexual exploitation and abuse, product design, data practices, and AI deployment as they affect children; due diligence obligations; monitoring and enforcement; effective regulation in contexts of limited regulatory capacity.*

Across the African region, legislative, policy, and regulatory measures are evolving to protect children's rights in digital environments. These interventions draw on regional frameworks such as the African Charter on the Rights and Welfare of the Child (ACRWC) which is a binding regional child-rights treaty that establishes protections relating to children's dignity, privacy, protection from abuse and exploitation.

The African Union Child Online Safety and Empowerment Policy (2024) provides a common framework for African Union (AU) member states to protect children's rights while enabling meaningful digital participation. It addresses online exploitation and abuse, privacy and identity, institutional capacity, corporate responsibility, digital literacy, research and cross-border cooperation.

The AU Strategy and Plan of Action against Online Child Sexual Exploitation and Abuse (2020–2025), this strategy aims to promote stronger criminal-justice systems, institutional coordination, prevention, victim support and international cooperation to address online child sexual exploitation and abuse.

On the other hand, the AU Data Policy Framework (2022) provides safeguards for children's personal data and recognises distinct risks they face in the digital environment, it also calls for policies and measures to identify and mitigate those risks, helping to protect children's privacy, safety, and rights online.

Frameworks governing AI's impact on children are still emerging across the continent although Africa has an AU Continental AI Strategy (2024) which promotes responsible, inclusive and development-oriented AI governance. It recognises risks including discrimination, privacy violations, surveillance, deepfakes and harms affecting vulnerable groups, including children. National AI strategies are also being developed at different rates, countries such as Kenya, South Africa, Rwanda but a strategy that promotes ethical AI is not equivalent to a law that creates enforceable obligations to protect children. A significant development is the African Commission on Human and Peoples' Rights' (ACHPR) Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age, adopted in May 2026. The Declaration expressly addresses generative AI, AI-generated sexualised images of children, chatbot-related risks, safety and privacy by design, and child-rights impact assessments.

7. What broader, more systemic interventions are needed in your country/region to address online harms?

*Consider: education, literacy efforts, mental health support, content moderation efforts, digital safety measures, adequate resourcing of policing and investigating crimes, taking down identified CSAM.*

1. Make awareness-raising and educational resources available to enable children, parents, and caregivers to make informed decisions about using an online service or product such Intervention have been exemplified by the Uganda Communications Commission which launched the Child Online Protection campaign at Kololo Secondary School (Monitor 2026, October) in Kampala, calling for stronger awareness, reporting and coordinated action to protect children from harm online.
2. Require technology companies and social media platforms to invest in content moderation capabilities for widely spoken African languages and regional dialects to catch localized abuse and grooming tactics.
3. Human rights due diligence is a core feature of the Guiding Principles on Business and Human Rights. Every business should undertake human rights due diligence in order to identify and manage the risks and impacts of its activities on children's rights within the digital environment.
4. Training law enforcement officers, cybercrime investigators, and members of the judiciary to handle sensitive digital crimes against children. This also calls for equipping national cybersecurity agencies and specialized police units with adequate budgetary support, digital forensics tools, and dedicated child protection desks. (Interpol,2026)
5. Strengthening cross-border legal cooperation under frameworks like the Malabo Convention and the AU Child Online Safety and Empowerment Policy (2022) to prosecute transnational perpetrators of online child exploitation.

8. How are States addressing their child rights obligations through legislative and regulatory approaches – for example, to ensure that digital tools and products used by children are safe and age-appropriate, and to ensure consistency with the human rights requirements of legality, necessity, and proportionality where rights are restricted?

*Consider: measures to promote age-appropriate design and child rights by design; age assurance approaches, and their implications for privacy and access to information; necessity, proportionality, and least intrusive means; and the use of child rights impact assessments to evaluate measures affecting children.*

Kenya's *Communications Authority's Industry Guidelines for Child Online Protection and Safety,* encourage age-related safeguards and measures to improve children's online safety. They require providers to apply safety and data protection by design, high default privacy settings, parental controls, age verification, and complaint systems. They also require device manufacturers to pre-activate parental controls before sale. The guidelines are built on nine principles, including the best interests of the child.

(ACERWC 2001). Statement of the Working Group on Children's Rights and Business on the 2024 World Safer Internet Day. African Committee of Experts on the Rights and Welfare of the

Child. The Working Group on Children's Rights and Business has called on businesses to conduct child-rights-based due diligence and embed safety-by-design and age-appropriate design.

9. How are States regulating age-inappropriate content, algorithmic amplification, and product liability in ways that protect children while respecting the full range of their rights?

*Consider: definitions of age-inappropriate content and liability frameworks; intermediary and product liability; algorithmic amplification; balancing child protection with freedom of expression and access to information. Across Africa, approaches include a combination of child-protection law, data-protection rules, regulatory guidelines and proposed age restrictions.*

States across Africa are navigating the complex task of protecting children from digital harms while safeguarding their fundamental rights and they have undertaken the following measures;

Many African countries through their laws are codifying harms children face online for example South *Africa's Films and Publications Amendment Act,* explicitly define age-inappropriate and harmful content. This includes sexually explicit material, online grooming, cyberbullying, self-harm promotion, and extreme violence.

Tanzania's *Communications Regulatory Authority under the Electronic and Postal Communications (Online Content) Regulations* mandate that internet service providers (ISPs) and online content hosts provide filtering mechanisms and parental control options to shield minors from harmful material. This provision supports measures such as restricting children's exposure to sexually explicit material, harmful content and other inappropriate online material.

Uganda's *Anti-Pornography Ac*t Cap 119 under Section 10 of the Act criminalises producing, participating in the production of, trafficking in, publishing, broadcasting, procuring, importing, exporting or otherwise aiding pornography depicting images of children. The Computer Misuse Act also lays down a punishment of 15 years imprisonment for any person who makes available child pornography for the purposes of its distribution through a computer.

Ghana's *Cybersecurity Act, 2020* requires internet service providers to deploy moderation, filtration, and reporting mechanisms to prevent predators from using them as a medium for facilitating offering or soliciting unlawful sexual conduct involving a child. If an operator becomes aware of child dealing on their platform and fails to intervene, they cross the legal line into complicity.

Gabon through its Ordinance No. 0011/PR/2026 requires platforms to filter algorithmic recommendations of AI-generated violent, sexual or psychologically harmful content for accounts identified as belonging to minors.

10. Have States adopted or proposed measures that would disproportionately impact human rights, such as online freedom of expression or privacy, with the stated aim – however well intentioned – of protecting children in the digital environment? If so, please provide specific examples.

*Consider: online content restrictions with vague language or unclear links to child protection, blanket restrictions on end-to-end encryption, disproportionate sanctions for online content or speech deemed harmful to children.*

African states have adopted or proposed measures intended to protect children online that also raise questions about freedom of expression, privacy, access to information and proportionality. Cases in point are blanket restrictions on end-to-end encryption and social-media age restriction

Gabon adopted *Ordinance No. 0011/PR/2026* which establishes a digital age of majority of 16 and introduces extensive obligations for social-media platforms. Minimum-age restriction can limit adolescents' access to educational information, peer-support networks, creative expression and civic participation. Age-verification systems can also create privacy risks if they collect excessive identity information. Parental-consent exceptions may create additional barriers for children without available or supportive caregivers.

Additionally, Rwanda is moving towards tightening laws on minors social media use targeting services such as Facebook, Instagram, and YouTube. Authorities are said to be considering the use of national digital ID to verify the age of users, equally raising questions and concerns of privacy on the personal information collected [EcoFin Agency, *Rwanda Considers Social Media Ban for Children Under 16*, 2026].

Zimbabwe has also approved its National Child Online Protection Policy to ensure children's protection from online abuse, cyberbullying and sexual exploitation, and which could be followed '...by measures to regulate or restrict minors' access to certain social media platforms' [The Besana Mail, *Zimbabwe approves landmark child online protection policy as digital risks to children grow*, 2026].

In March (as of Techdesk Africa's report), Nigeria launched a public consultation on the proposed draft age restrictions. 'The findings showed that over 80 percent of Nigerians support age regulation, with 64.5 percent specifically favouring a minimum social media cut-off age of 16 or 17' [The Guardian Nigeria, *Kids on social media: Balancing digital access, child safety amid new guardrails*, 2026; Techdesk Africa, *Nigeria starts considering social media age restrictions with public consultation,* 2026]. Meanwhile, time will tell as to how well such measures balance with children's broader rights and freedoms.

Egypt has also moved towards similar bans whereby '...platforms are strictly forbidden from allowing children under 13 to create or activate independent personal accounts' [Egypt Independent, *Egypt bans social media accounts for under-13s and mandates "safe mode" for ages 13-15*, 2026].

**Responsibilities of business enterprises**

11. What concrete measures have companies (or your company) implemented to meet their responsibility to respect children's rights under the UN Guiding Principles on Business and Human Rights and the Children's Rights and Business Principles, including with regard to AI products and services?

*Consider: child rights by design; human rights due diligence and child rights impact assessments before deployment; transparency and public reporting; responsibilities of those who profit from digital spaces to prevent harms*.

Under the UN Guiding Principles on Business and Human Rights and the Children's Rights and Business Principles, companies have a responsibility to respect children's rights throughout their operations, products, services and business relationships.

MTN Uganda partnered with the Internet Watch Foundation, Meta, the International Centre for Missing and Exploited Children and Child Helpline International, with the support of the United Nations office on Drugs and Crime (UNODC), to launch the Help Children be Children campaign and the Child Safety Online Africa Portal to increase public awareness of the impact of Child Sexual Abuse Material and help prevent its spread in target countries on the African continent.

Africell launched Kidzonet in The Gambia, a SIM-based child online protection service designed to help children access the internet safely while limiting exposure to harmful and age-inappropriate content. Kidzonet operates directly at the SIM level, requiring no mobile applications or complex device configurations.

12. What accountability and remedy mechanisms provided by companies are proving most promising, and where are the greatest gaps, including across companies of different sizes and those operating across multiple countries and regions?

*Consider: access to remedy where harm occurs, and its accessibility to children and families; regulatory accountability; responsibilities of regional companies and SMEs alongside global platforms*.

Under the UN Guiding Principles on Business and Human Rights, companies should provide a remedy when they cause or contribute to adverse human rights impacts. States must also ensure access to effective judicial and non-judicial remedies. Companies are increasingly adopting promising accountability and remedy mechanisms like embedding "child rights by design," implementing transparent content moderation, and investing in digital literacy, which help prevent harm and empower users.

However, significant gaps remain, particularly for smaller companies lacking resources and expertise. Larger, multinational corporations often exhibit inconsistent policy enforcement across regions, algorithmic blind spots, and opaque appeals processes. The cross-border nature of operations creates further challenges, with varying legal frameworks, cultural nuances in content moderation, jurisdictional complexities for enforcement, and limited effective age assurance

methods that balance privacy and access to information, leaving many users, especially children and those in less regulated regions, with inadequate recourse when harm occurs.

Human rights due diligence is a core feature of the UNGPs. Every business should undertake human rights due diligence in order to identify and manage the actual or potential human rights - including child rights - risks and impacts that its activities or business relationships could cause, contribute to, or be linked to. This requires policies and processes aimed at the implementation of risk management measures.

**The gaps**

Children mostly do not use formal channels. For instance, in the Uganda report only 19% of children felt confident reporting harmful content on social media, and the IWF portal had received just 13 reports by 2019. Global platforms cannot be compelled by Ugandan courts and may disclose non-content data only voluntarily, and Ugandan authorities made just three requests for user data to global platforms in 2017-2019.

Additionally, Meta argued Kenyan courts lack jurisdiction where it is not registered. The Kenyan courts rejected that for the cases concerned, but it shows how absence of local presence can limit accountability.

The current reliance on English-centric moderation tools is a significant operational failure in markets with high linguistic diversity. In many African regions, harmful content including incitement to violence and child exploitation is often circulated in local languages that bypass automated safety filters. Because AI classifiers and human moderators lack proficiency in these languages, harmful content remains undetected for longer periods, and user reports in local languages are often ignored or miscategorized. To truly meet their 'duty of care,' industry actors must move beyond translation tools and invest in native-language moderation and culturally nuanced AI training sets.

**Digital safety, privacy, and the rule of law**

13. How can children’s protection from sexual exploitation and abuse be pursued in ways that are consistent with guaranteeing the right to privacy and access to secure communications for all?

*Consider: approaches to preventing and responding to child sexual exploitation and abuse in the digital environment that are consistent with the protection of privacy and secure communications, including how the requirements of legality, necessity and proportionality are applied in practice.*

The rights-based approach (RBA) offers a unique and practicable framework to address children’s rights holistically while recognising their multiple vulnerabilities, needs, and contexts across the continent. Central to the approach is the notion of human rights and equality as an integral part of development; human development. Congizant of UN’s *Ten Key Steps for Regulations to Protect Children Online*, and blended with the Survivor-centric Approach, the approach offers mechanisms to ensure participation, accountability and non-discrimination mechanisms across policy and decision-making processes, as well as AI systems (from design-to-governance) at all levels to ensure children’s online protection and safety. This, among other things, would

encompass robust and child-centric legal measures, including criminalising OCSEA and TFGBV (and covering the specific risks and threats young girls face) through domestic judicial systems, localising and sensitizing domestic laws, investing in tailored digital literacy programs, fostering multi-stakeholder collaboration and partnership to ensure the installation of accessible, affordable and safe reporting, and psycho-social support mechanisms for child survivors of online harms at the national and sub-national levels [ECPAT et al., *Girls & Young Women-Led Assessment on Online Sexual Exploitation, Abuse & Technology-Facilitated Gender-Based Violence in Africa*, 2025].

Additionally, it also entails creating an enabling environment for children to share their lived experiences and views, including on how to best accommodate and rehabilitate children survivors and ensure durable solutions to online harms for generations to come. In turn, this demands an environment where their rights and freedoms are respected and protected, including that of access to information, expression, safe access to the internet and digital platforms, as well as protection from the threat or actual retaliation if and when they do speak out against such harms.

14. How can children be protected from abuse without over-criminalizing their own conduct, consistent with due process protections and the principle of evolving capacities?

*Consider: peer-to-peer conduct and developmentally typical behavior; the best interests of the child in justice processes; and due process protections.*

1. Prioritizing the Best Interests of the Child

Consistent with the UNCRC General Comment No. 25, justice processes should prioritize support and rehabilitation over punishment for minors. The Survivor-Centric Approach is guided by human rights principles and seeks to ensure that responses do not cause further harm or re-traumatization. This approach to justice goes beyond allowing children to file complaints. It ensures they are treated with dignity, heard and protected throughout the process, and can obtain effective remedy.

**Key Principles of the survivor centered approach**

- **Safety**: Prioritize the survivor's physical, emotional, and digital safety.
- **Confidentiality**: Protect personal information and respect privacy.
- **Informed Consent**: Obtain permission before taking action or sharing information.
- **Respect**: Treat survivors with dignity and compassion.
- **Non-Discrimination**: Provide support without bias or judgment.
- **Survivor Autonomy:** Respect the survivor's choices and decisions.
- **Non-punishment of child victims**. The UN Committee on the Rights of the Child (CRC Committee) adopted its comprehensive Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography stress that children should never be held responsible for sharing self-produced sexual material. Law should provide express immunity for children coerced, groomed or exploited into producing or sharing content, and for children who disclose abuse.

The distinction between ‘online’ and ‘offline’ is often blurred. Online exploitation and abuse can stem from sexual abuse perpetrated in the physical world, which is documented and shared using digital technology. However, online services can also be used to connect with the child with the intent to harm them in person or through digital technology.

Legal frameworks must sharply distinguish between genuine abuse (such as adult grooming, coercion, extortion, and non-consensual image distribution by bad actors) and consensual or exploratory adolescent peer conduct. Treating typical adolescent behavior under severe child sexual abuse material (CSAM) laws exposes minors to lifelong criminal records, stigmatization, and severe psychological harm.

**International cooperation and options for a framework**

15. What are the most critical gaps in addressing children's rights in the digital environment through international cooperation, and what forms of cooperation are most urgently needed?

*Consider: gaps between existing instruments, standards, and their implementation; coordination between States, international organizations, the private sector, and civil society; support for countries with differing levels of regulatory capacity; and responsiveness to rapid technological change.*

International cooperation faces some critical challenges. Among others, the disparities and differences between the states (contextual, cultural, legislative, institutional, financial, technical, and technological) (especially that of the Global South); the speed at which emerging technologies are evolving, and the risks posed against children; big tech’s monopolies of power and profit-first thinking which has oriented the trajectory of influence pathways in decision and policy-making processes, the lack of consensus on what ‘the best interest of the child’ means in practical terms (arguments for and opposed the social media use ban to children under the age 16 are cases in point), resource allocation schemes leaning towards power as opposed to ‘value’ (especially that of children’s life, survival, and development), the absence of children’s voice in discourses on matters affecting them, and the increasing shrinking of the civic space are among the most pressing.

In this regard, cooperation which centers children, meaningfully engages them, respects their voices and responds to their views tangibly in areas that matter most to their lives, development, and survival, and ensures the integration of their diversities, lived experiences, vulnerabilities, as well as rights and freedoms in global, continental, and national-level processes is both urgent and critical. Moreover, to ensure sustainability, cooperation ought to build on existing initiatives, as opposed to duplicating them, integrating efforts to curtail siloed interventions and promoting harmonization at the continental and national levels, embed children’s digital rights within broader developmental plans and support localisation by facilitating nationally-led initiatives, and ensuring inclusive platforms and spaces for the Global South to engage in global discourse, grass-root initiatives to showcase best practices, and facilitating opportunities for collective advocacy by key stakeholders across sectors for children’s digital rights.

16. What options for a framework, including at the global level, should be considered to advance children's rights and safety in the digital environment? How might they relate to existing instruments and processes?

*Consider: the forms such options might take; the respective roles of States, business, and international organizations; implementation and accountability; and how any suggested options would add value to, rather than duplicate, existing efforts.*

1. **Member states to,**
    - Develop and enact child-centered national laws that protect children's privacy and safety in digital spaces, cognizant of the rights-based approach, best interest, views, contexts, and vulnerabilities to counter online harms;
    - Embed child digital rights within broader development priorities and commitments;
    - Mainstream digital literacy programs in education programs, community engagement, and cross-sector capacity-building initiatives to meet the implementation gaps;
    - Train law enforcement officers, cybercrime investigators, and members of the judiciary to handle sensitive digital crimes against children effectively which also calls for equipping national cybersecurity agencies and specialized police units with adequate budgetary support, digital forensics tools, and dedicated child protection desks;
    - Criminalising 'micro-targeting' of children for commercial purposes and applying targeted age-restrictions to certain harms;
    - Embedding compliance to human and children's rights due diligence by companies and strict data collection, storage, and use guardrails to curb privacy risks related to age-verification processes;
    - Require technology companies and social media platforms to invest in content moderation capabilities for widely spoken African languages and regional dialects to catch localized abuse and grooming tactics;
    - Ensuring meaningful engagement of children themselves in key decision and policy making processes;
    - Installing and implementing evidence-driven accountability and transparency mechanisms to ensure effective redress to child survivors;
    - Strengthening cross-border legal cooperation and collaborating with CSOs, governments, academia, media and other key stakeholders on evidence-generation, awareness raising, capacity-building, and advocacy initiatives.
2. **Platforms and telecom companies to,**
    - Comply with human and children's rights due diligence;
    - Design and deploy child-friendly products and services;
    - Minimise the collection and retention of children's data;
    - Introduce age verification and parental controls;
    - Publish transparency reports, information on content moderation practices, and submit protection measures to independent audits;

- Collaborate with CSOs, governments, academia, media and other key stakeholders on evidence-generation, awareness raising, capacity-building, and advocacy initiatives.

3. **The media to,**
    - Objectively and ethically monitor, document, and report;
    - Expose all cases of online child abuse and demand accountability from the responsible parties; and
    - Collaborate with other key stakeholders on evidence-generation, awareness raising, capacity-building, and advocacy initiatives.
4. **Civil society organisations to,**
    - Engage in research and evidence-based advocacy through mainstream and social media platforms;
    - Support digital literacy initiatives;
    - Provide technical inputs geared towards legal and institutional reforms;
    - Document and report issues affecting child safety online in order to demand and push for accountability of all the relevant stakeholders;
    - Provision of legal aid and psycho-social support services for child survivors (or facilitating referrals); and
    - Collaborate with other key stakeholders on evidence-generation, awareness raising, capacity-building, and advocacy initiatives.
5. **Academia and Researchers to,**
    - Inform policy and programmatic dialogues through evidence-generation and dissemination;
    - Provide technical inputs in digital literacy programs and initiatives;
    - Collaborate with other key stakeholders on evidence-generation, awareness raising, capacity-building, and advocacy initiatives.
6. All stakeholders must ensure that children are meaningfully engaged, consulted, and informed in all matters affecting them, parents and guardians are capacitated across discussions, collaborations, and co-design of digital solutions.

[Also see DRAA website, https://digitalrightsalliance.africa/; and Report on *Child Protection and Safety Online in Africa,* 2025]