

# THE AFRICAN UNION CHILD ONLINE SAFETY AND EMPOWERMENT POLICY







# **THE AFRICAN UNION CHILD ONLINE SAFETY AND EMPOWERMENT POLICY**

Adopted by the 44<sup>th</sup> Ordinary Session of the African  
Union Executive Council  
February 2024 - Addis Ababa, Ethiopia

## TABLE OF CONTENTS

<b>GLOSSARY OF DEFINITIONS .....</b>	<b>2</b>
<b>I. EXECUTIVE SUMMARY .....</b>	<b>4</b>
<b>II. INTRODUCTION .....</b>	<b>5</b>
<b>III. BACKGROUND .....</b>	<b>5</b>
III.I ACCESS TO THE DIGITAL WORLD FOR CHILDREN IN AFRICA .....	5
III.II THE OPPORTUNITY .....	6
III.III THE RISKS .....	6
III.IV FACTORS INFLUENCING CHILD ONLINE SAFETY .....	8
III.V EXISTING FRAMEWORKS AND TOOLS FOR CHILD ONLINE PROTECTION IN AFRICA .....	8
<b>III. GUIDING PRINCIPLES .....</b>	<b>10</b>
<b>IV. POLICY GOALS .....</b>	<b>11</b>
<b>V. IMPLEMENTATION PLAN.....</b>	<b>12</b>

## GLOSSARY OF DEFINITIONS

Term	Definition
AU Agenda 2063	The blueprint and master plan for transforming Africa into the global powerhouse of the future.
AU Continental Education Strategy for Africa (CESA) 2016-2025	The strategy aims to reorient Africa's education and training systems to meet the knowledge, competencies, skills, innovation and creativity required to nurture African core values and promote sustainable development at the national, sub-regional and continental levels.
AU Digital Transformation Strategy	A comprehensive ten years (2020-2030) forward looking strategy that aims at harnessing the potential of digital technologies, data and innovation to accelerate the transformation of today's Africa to the peaceful, integrated and prosperous Africa.
Child	Any person under the age of 18, as per the United Nations Convention on the Rights of the Child.
Child Sexual Abuse Material (CSAM)	<p>Imagery or videos which show a child in a sexualised manner, engaged in or depicted as being engaged in explicit sexual activity.</p> <p>NB This terminology replaces the previously used term "child pornography", which is now widely accepted to be inaccurate and fails to capture the harm inherent in this act.<sup>1</sup></p>
Corporate Social Responsibility	Corporate social responsibility (CSR) is a self-regulating business model that helps a company be socially accountable—to itself, its stakeholders, and the public.
Cyber-aggression	Acts of harm enacted by individuals or groups, online or through the use of digital technology, often with the intention of causing offense or hurt to another individual or group.
Cyber-bullying	Includes sending, posting, or sharing negative, harmful, false, or mean content, including personal or private information about an individual or a group of individuals, in order to cause embarrassment or humiliation.
Digital accessibility	Digital accessibility is the ability of a website, mobile application or electronic document to be easily navigated and understood by a wide range of users, including those users who have visual, auditory, motor or cognitive disabilities.

<sup>1</sup> See INHOPE: What is Child Sexual Abuse Material? <https://www.inhope.org/EN/articles/child-sexual-abuse-material>

Digital platform	A software-based online infrastructure that facilitates interactions and transactions between users
Digital skills	A set of skills, tools, and knowledge necessary to use networks, digital devices and different applications on online media that facilitate the management of information according to specific requirements of working environment, learning environment, and problems solving situations.
Digital environment	All websites, services, apps and other forms of spaces accessed using technology.
General comment No. 25	The United Nations Committee on the Rights of the Child clarification of how the Convention on the Rights of the Child applies in the digital environment.
Harm	A negative impact upon a person, such as financial, physical, or emotional damage.
Online Child Sexual Exploitation	The use of technology or the internet to facilitate the sexual abuse of a child, including the production and sharing of child sexual abuse material online.
Personal Data	Any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier or to one or more factors specific to physical, physiological, mental, genetic, economic, cultural or social identity of that person.
Risk	A situation or set of factors that has the potential to cause harm. Through the identification of 'risks', harm may be mitigated or prevented.



## EXECUTIVE SUMMARY

Access to the digital space in Africa is increasingly expanding, and many of those coming online are children –defined as ‘all those under the age of 18’. It is estimated that worldwide 1 in 3 internet users is a child, and more than 175,000 children go online for the first time every day - a new child every half second.

In Africa it is estimated that 40% of youth aged between 15-24 years can access the internet. With children getting connected to the digital world so too the risks that the online world brings to children have grown. The Covid-19 pandemic increasingly drew African children to the online world, with some accessing the internet for the first time. Online risks are present 24/7 through devices that enable access to the internet. The situation is exacerbated for children with special needs and disabilities. The international child rights community categorises online risks to children into 4 categories – content, contact, conduct and consumer/contract risks (4Cs).

The African Union Child Online Safety and Empowerment Policy assessed the landscape in terms of the associated opportunities and risks in the cyberspace for African children. It outlines key guiding principles anchoring the protection of children in the online environment, identifying key policy goals in the African context and charting out an implementation plan to assist the African Union and its member states with the realization of the policy goals and objectives.

When developing national policies on child online protection, policy makers should bear certain guiding principles in mind to steer policy development. These principles have been underscored in UNCRC General comment No. 25 (2021) on children’s rights in relation to the digital environment and the General comment No. 7 on Article 27 of the African Committee of Experts on the Rights and Welfare of the Child (ACERWC) articulating four guiding principles, including: i) best interests of the child; ii) non-discrimination to close the gender-related digital divide for girls; iii) right of a child to life, survival and development; and iv) participation of children to express their views and offer training and support for children to participate on an equal basis with adults, anonymously where needed.

To realize child safety and empowerment, the Policy sets the following objectives and the strategic imperatives for a comprehensive national action plan for the protection of children online, namely: institutional capacity development; legal and regulatory frameworks; Personal data, privacy and identity protection of a child; response and support systems against child exploitation and abuse (CSEA); corporate responsibilities of businesses to uphold children’s rights; training and education across the value chain; raising public awareness and communications of online risks; research and development in the child safety area; and most importantly fostering international cooperation to exchange good practices and lessons learned.

Amongst the key recommendations of the policy is the need to affirm strong commitments to child online safety at the highest level in government; strengthening criminal justice frameworks to enable law enforcement and the judiciary to effectively tackle child online safety related offences including child online sexual exploitation and abuse (CSEA); promoting and supporting accessible digital education in schools and for parents, guardians and community leaders; developing and maintaining databases to pool resources and information exchange including hotlines for reporting and victim support; and establishing an African child online resource fund and program.

The Policy calls for a whole society approach to be employed for implementation due to the cross-sectoral, cross-border and transnational nature of the digital environment necessitating strong national, regional, and international cooperation to mitigate the risks arising from the misuse of digital technologies, to ensure that all stakeholders, including States, businesses, and other actors, effectively respect, protect and fulfil children’s rights in relation to the digital environment. The need for gathering rigorous data that would lead to development of future evidence-based interventions that strengthen online safety for children with proper attention to all aspects of child rights that are impacted in this digital age. The policy, and its proposed implementation plan, has been designed to assist African Member States with the development of national child online safety and empowerment policies as well as paving the way for a safer and nurturing online environment for children to ensure an inclusive digital society and economy with active participation of Africa’s future generation, the children.

## I. INTRODUCTION

The digital world holds great promise for Africa and in particular for our children – but alongside its myriad opportunities it also presents risks. Children, defined as all those under the age of 18, have established rights grounded in the UN Convention on the Rights of the Child<sup>2</sup> – ratified by every country on the African continent – that must be protected, online<sup>3</sup> and offline equally. As more children go online in Africa – a trend promoted by the global campaign of broadband access for all and hastened by the Covid-19 lockdown and curfew measures – it is critical to ensure the digital environment is a space where children can thrive.

It is in this context that the African Union (AU) Commission is spearheading the development of an AU Child Online Safety and Empowerment (the Policy). The Policy will provide a strong framework for the implementation of children's existing rights in the digital environment, including by the private sector and other stakeholders making products or offering services likely to be accessed by children. It will support Member States to maximize the benefits of children's use of Information and Communication Technologies (ICTs) while minimizing the risks, always prioritising the best interests of the child.

The AU Child Online Safety (COS) and Empowerment Policy seeks to identify gaps and areas where harmonisation is needed to implement children's rights address cross-border challenges. It will provide national policy-makers and regulators with a framework that ensures ICT providers respect children's rights; equip children, parents/guardians, educators, social service agencies/organizations, industry, and law enforcement officials in Africa with the right tools and skillsets to ensure children's safety in the online environment; and lay the groundwork for ongoing research and evidence-gathering to ensure the contextualisation of implementation to the African context. This Policy provides:

1. A common set of principles, goals and assessment criteria for COS, based on international best practice;
2. A multi-stakeholder framework<sup>4</sup> for national policy-makers to implement COS policies;
3. A set of priority actions for implementation at AU level.

The Policy should be understood and implemented in conjunction with other related AU strategies and legislation, notably the African Charter on the Rights and Welfare of the Child<sup>5</sup> and the African Union Convention on Cybersecurity and Personal Data.<sup>6</sup>

## II. BACKGROUND

### Access to the digital world for children in Africa

Access to the digital world in Africa is expanding, and many of those coming online are children. It is estimated that worldwide 1 in 3 internet users is a child,<sup>7</sup> and more than 175,000 children go online for the first time every day – a new child every half second. In Africa it is estimated that 40% of youth aged between 15-24 years can access the internet.

Children are among the most enthusiastic explorers of technology. In a study conducted in South Africa<sup>8</sup> in 2016 targeting children aged 9-17 and their parents found that:

---

<sup>2</sup> UN Commission on Human Rights, Convention on the Rights of the Child, 7 March 1990:

<https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>

<sup>3</sup> How the Convention applies in the digital environment is set out in UNCRC General comment No. 25 (2021):

[https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en)

<sup>4</sup> In compliance with UNSDG 2020, Common Minimum Standards for Multi-stakeholder Engagement:

<https://unsdg.un.org/sites/default/files/2020-05/UNSDG-Common-Minimum-Standards-for-Multi-Stakeholder.pdf>

<sup>5</sup> <https://au.int/en/treaties/african-charter-rights-and-welfare-child>

<sup>6</sup> <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

<sup>7</sup> UNICEF, The State of the World's Children 2017: <https://www.unicef.org/reports/state-worlds-children-2017>

<sup>8</sup> Global Kids Online, South African Kids Online: A glimpse into children's internet use and online activities (2016): <http://globalkidsonline.net/southafrica/>



- 70.4% of the children interviewed used the internet as opposed to 65.8% of the interviewed parents;
- 46.0% of those that used it could access the internet whenever they wanted.

As expansion into the digital world continues, the need for Africa to consider child safety by design and default becomes ever more urgent.

## The opportunity

Digital accessibility furnishes children with enormous opportunities and diverse development outcomes, based on its usage. Access to the internet can help children stay connected, improve their digital literacy, enhance educational emancipation and diversify their livelihoods. With increasing digitalization, children are now able to access e-education tools, connect with peers and utilize the enormous potential the internet provides to them. The digital environment can positively contribute to children's rights, including the rights to be heard, to express themselves, to associate with others, to enjoy their privacy, to seek information, and to play, as set out in the United Nations Convention on the Rights of the Child. The 2016 South African study found that socialising, especially via instant messaging, learning and school-work were popular activities among internet users with 95.6% reporting that they sometimes or always had fun when they went online.

The use of digital technology is a key driver of change that fosters the realization of the African Union Digital Transformation Strategy,<sup>9</sup> the AU Agenda 2063 Aspirations,<sup>10</sup> the Africa's Agenda for Children 2040: Fostering an Africa Fit for Children;<sup>11</sup> and partly underpins the realization of the Sustainable Development Goals (SDGs).<sup>12</sup> Improving access to affordable data and devices for children is critical to delivering on the promised opportunity.

## The risks

As children access the digital world so too the risks that the online world brings to children have grown. The Covid-19 pandemic has increasingly drawn African children to the online world, with some accessing the internet for the first time. Online risks can be present 24/7 through devices that enable access to the internet. The situation can be exacerbated for children with special needs and disabilities.

The international child rights community categorises online risks to children into 4 categories – content, contact, conduct and consumer/contract risks, as outlined in figure 1 below:

<sup>9</sup> <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>

<sup>10</sup> <https://au.int/en/agenda2063/goals>

<sup>11</sup> African Committee of Experts on the Rights and Welfare of The Child (ACERWC), Nov 2016: [https://au.int/sites/default/files/newsevents/agendas/africas\\_agenda\\_for\\_children-english.pdf](https://au.int/sites/default/files/newsevents/agendas/africas_agenda_for_children-english.pdf)

<sup>12</sup> <https://sdgs.un.org/goals>


	<b>Content</b> Child engages with or is exposed to potentially harmful content	<b>Contact</b> Child experiences or is targeted by potentially harmful <i>adult</i> contact	<b>Conduct</b> Child witnesses, participates in or is a victim of potentially harmful <i>peer</i> conduct	<b>Contract</b> Child is party to or exploited by potentially harmful contract
<b>Aggressive</b>	Violent, gory, graphic, racist, hateful or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
<b>Sexual</b>	Pornography (harmful or illegal), sexualization of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
<b>Values</b>	Mis/disinformation, age-inappropriate marketing or user-generated content	Ideological persuasion or manipulation, radicalisation and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
<b>Cross-cutting</b>	<b>Privacy violations</b> (interpersonal, institutional, commercial) <b>Physical and mental health risks</b> (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) <b>Inequalities and discrimination</b> (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

Figure 1: The 4Cs, from Children Online: Research and Evidence 2021<sup>13</sup>

The 2016 South Africa study found:

- One in three child participants had been exposed to hate speech (34.5%) and to gory images (32.7%) online.
- More than one in five of all child internet users (21.9%) reported having been treated in a hurtful or nasty way in the past year (either face to face or online).
- 41.2% said that they had at least once in their lifetime had contact with someone online that they had never met face to face before.
- 54.0% of those who had first met someone online indicated that they went ahead to meet them face to face.
- When asked if they had seen any sexual images online in the past year, 51.2% of child participants reported that they had and one in three had received a sexual message (30.5%). One in five (20.5%) child participants had been sent a message they did not want with advertisements for or links to X-rated websites, 19.2% opened a message or a link in a message that showed pictures of naked people or of people having sex that they did not want and 20.3% had seen or received a sexual message, image or video about someone else that they did not want.

<sup>13</sup> <https://doi.org/10.21241/ssoar.71817>

The findings of a similar study done in Ghana in 2017 mirrored those obtained from the South African study.<sup>14</sup> Further studies from Kenya have also highlighted the mental health<sup>15</sup> and sexual exploitation risks<sup>16</sup> that are rapidly increasing for children.

## Factors influencing child online safety

Many factors combine to influence child safety online.

1. **The global nature of the digital environment** brings with it shared challenges and opportunities for action. The tech sector operates simultaneously across many different legal jurisdictions. The development of shared international approaches to the regulation of the private sector and a cross-border community of best practice for education, enforcement and victim support amongst others, can provide effective responses.
2. **The design of ICT products and services** is critical, as commercial interests, if not adequately adjusted in view of the rights of the child, can create or reinforce risks to children's safety. Safety by design strategies backed up by law have been found to be a fundamental driver toward tech sector product safety – particularly in relation to children.
3. **Children's overall well-being** affects how they engage with the internet. Evidence shows that children who are vulnerable offline are also more likely to be vulnerable online, hence protective offline factors can also reduce exposure to online risks. Offline factors that create vulnerability or protection influence how children engage with the online environment. Local, offline interventions are therefore also required as part of a holistic strategy.
4. Similarly, **knowledge and support from parents/guardians, educators and peers** can help children to become more confident internet users.<sup>17</sup> Some exploratory studies suggest that social support and children's positive relationships with the people around them can act as protective factors, arguing that protecting children online is more efficient when combined with supportive parenting offline.

## Existing frameworks and tools for child online protection in Africa

There are national, regional and continental initiatives, frameworks and tools relevant to child online safety in Africa. They are however focused largely on the most heinous of abuses, notably child sexual exploitation and abuse, and in particular on victims' rights. The wider context and in particular the role of companies and system design is a prominent gap.

### 1. National

While roughly 52%<sup>18</sup> of African countries have some sort of data and privacy protection legislations in place (including limited protection in other laws), the majority of those legislations are either limited in scope and applicability to children's online environment or yet to be fully enforced. **Child-focused data**

---

<sup>14</sup> [Risks and Opportunities related to Children's Online practices, Ghana country report 2017](https://www.unicef.org/ghana/media/1791/file/Risks%20and%20Opportunities%20-%20Child%20Online%20Protection.pdf). This study targeted 3000 children aged between 9 - 17 and 1000 guardians/parents. <https://www.unicef.org/ghana/media/1791/file/Risks%20and%20Opportunities%20-%20Child%20Online%20Protection.pdf>

<sup>15</sup> Kenya Paediatric, Adolescents in the Digital Age: <https://www.kenyapaediatric.org/wp-content/uploads/2018/05/Adolescents-in-the-digital-age-Dr.-Claire-Majisu.pdf>.

<sup>16</sup> Terre des Hommes, The Dark Side of the Internet for Children. Online Child Sexual Exploitation in Kenya – A Rapid Assessment Report (2018): <https://www.datocms-assets.com/22233/1600704755-tdh-nl-ocse-in-kenya-research-report-feb-2018.pdf>

<sup>17</sup> See the [South African study](#) for statistics on parents' impressions of the children's internet experiences, and on children's likelihood of communicating with their parents about online issues.

<sup>18</sup> UNCTAD Data Protection and Privacy Legislation Worldwide: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

***protection regulation has strong potential to address many of the risks faced by children online.<sup>19</sup>***

Many countries broadly address sexual exploitation or ban pornography in general; however, these laws are not enough as they do not specifically address the criminal aspects of various forms of online child sexual exploitation and abuse. Furthermore, the lack of a harmonized definitions, approach and legislative measures among Member States, pose a considerable challenge in making sure offences are identified as well as offenders tracked – including outside national borders – and eventually brought to justice.

There are already several examples of child online safety initiatives across Africa to draw inspiration from. Some countries have documented safety initiatives such as Kenya,<sup>20</sup> Ghana,<sup>21</sup> Uganda<sup>22</sup> and Zambia.<sup>23</sup> Expert organizations exist across Africa to guide thought on online safety, including the Africa Digital Rights Hub,<sup>24</sup> CIPESA<sup>25</sup> and Research ICT Africa<sup>26</sup>. Finally, there are examples of legislation within Africa to guide policy-making: Ghana's Cybersecurity Act<sup>27</sup> criminalized online sexual conduct with children and imposed obligations on telecommunications services; and Rwanda has a well-developed policy on child online protection,<sup>28</sup> together with a detailed five-year action plan.

## **2. Regional**

At the regional level, several child protection policies and legal frameworks are in place, inter alia: EAC Child Policy<sup>29</sup> & Framework for Strengthening Child Protection Systems in the East African Community<sup>30</sup>, SADC's Model Law on Eradicating Child Marriage<sup>31</sup> and in 2019 ECOWAS adopted a Child Policy and its Strategic Action Plan (2019-2023). Once again, the lack of harmonized regional frameworks is a major stumbling block for a coherent approach to child online safety on the continent and ultimately across the globe.

Once again, these laws reflect pre-digital safety concerns and do not extend to a more holistic and systemic approach to child online safety

## **3. Continental**

At the continental level, the African Charter on the Rights and Welfare of the Child was adopted in 1990 and entered into force in 1999. An African Union Committee of Experts on the Rights and Welfare of the Child (ACERWC) was established. The Committee's functions include the promotion and protection of the rights enshrined in the Charter. The Committee in 2019 adopted a declaration on preventing and ending online Child Sexual Exploitation in Africa.<sup>32</sup>

---

<sup>19</sup> The positive impact of robust data protection rules is evidenced by the changes made by tech companies in order to comply with the UK's Age Appropriate Design Code, which came into force in 2021: "[Children are better protected online in 2022 than they were in 2021](#)" - ICO marks anniversary of Children's code, Information Commissioner's Office, 2<sup>nd</sup> September 2022

<sup>20</sup> ITU, Status on Child Online Safety Initiative in Kenya: [https://www.itu.int/en/ITU-D/Documents/ChildOnlineSafetyInitiative\\_Kenya.pdf](https://www.itu.int/en/ITU-D/Documents/ChildOnlineSafetyInitiative_Kenya.pdf)

<sup>21</sup> Ghana, Be cyber smart - Tips to keep children safe online (7-10 years): <https://home.kpmg/gh/en/home/insights/2020/04/Be%20cyber%20smart%20tips%20to%20keep%20children%20safe%20online%207-10%20years.html>

<sup>22</sup> [www.stopit.ug](http://www.stopit.ug)

<sup>23</sup> [www.stopit.ac.zm](http://www.stopit.ac.zm)

<sup>24</sup> <https://africadigitalrightshub.org>

<sup>25</sup> <https://cipesa.org>

<sup>26</sup> <https://researchictafrica.net>

<sup>27</sup> Ghana Cyber Security Act – Act 1038, 2020

<sup>28</sup> [Rwanda Child Online Protection Policy](#), 2019

<sup>29</sup> EAC Child Policy, 2016: <http://repository.eac.int/bitstream/handle/11671/2013/EAC%20Child%20Policy.pdf?sequence=1&isAllowed=y>

<sup>30</sup> EAC Framework for Strengthening Child Protection Systems, 2017:

<file:///C:/Users/suliemana/Downloads/EAC%20Framework%20Child%20Protection%202018.pdf>

<sup>31</sup> SADC Model Law on Eradicating Child Marriage, 2016: <https://www.childrenandaids.org/node/1139>

<sup>32</sup> <https://acerwc.africa/sites/default/files/2022-07/ACERWC-33nd-Session-Draft-Report-English-Final-1.pdf>

The African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention),<sup>33</sup> has content related offences on child pornography incorporated in its articles. As such, there will be a looming requirement to introduce an amendment to the Convention to support the full realization of the rights of the child in the digital environment and protect children against all forms of online violence and harms.

There are also toolkits to support children safety online such as those of Child Online Africa.<sup>34</sup>

### III. GUIDING PRINCIPLES

When developing national policies in child online protection, policy makers should bear certain guiding principles in mind to steer policy development. These principles, which underpin also this continental policy, fall into two categories: the application of children's established rights, and accounting for cross-cutting issues.

#### 1. Apply children's established rights

The UNCRC General comment No. 25 (2021) on children's rights in relation to the digital environment and the General comment No. 7 on Article 27 of the African Committee of Experts on the Rights and Welfare of the Child (ACERWC) share four guiding principles:

- a) **Best Interests of the Child:** Member States are encouraged to ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration. In considering the best interests of the child, all children's rights must be regarded, including their rights to seek, receive and impart information, to be protected from harm and to have their views given due weight, and ensure transparency in the assessment of the best interests of the child and the criteria that have been applied.
- b) **Non-discrimination:** Member States are urged to take proactive measures to prevent discrimination on the basis of race, colour, national origin, citizenship, ethnicity, profession, political opinions, and any other opinions, and health including HIV status, disability, age, religion, culture, marital status, socio-economic status, status as a refugee, migrant, or any other status, sex, gender, or any other factor that could lead to discrimination against them. Specific measures will be required to close the gender-related digital divide for girls and to ensure that particular attention is given to access, digital literacy, privacy and online safety.
- c) **Right to life, survival and development:** Member States are exhorted to take all appropriate measures to protect children from risks to their right to life, survival and development.
- d) **Participation of children:** Member States are encouraged to promote awareness of, and access to, digital means for children to express their views and offer training and support for children to participate on an equal basis with adults, anonymously where needed. When developing legislation, policies, programmes, services and training on children's rights in relation to the digital environment, Member States are urged to involve children, listen to their needs and give due weight to their views. They should ensure that consultative processes are inclusive of children who lack access to technology or the skills to use it.

---

<sup>33</sup> AU Convention on Cybersecurity and Personal Data Protection, 2014: [https://au.int/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf). The Convention has not yet entered into force as so far 10 Member States of the required 15 have ratified the Malabo Convention

<sup>34</sup> <https://toolkits.childonlineafrica.org>



## 2. Account for cross-cutting issues

When it comes to the more practical drafting work, policy makers must also assess efforts to address the following cross-cutting issues:

- a) **Identifying risk and mitigating harm:** The first priority in child online protection must be to clearly identify the source of harms to children online and establish effective mechanisms for mitigating harms.
- b) **Promoting access, accessibility and inclusion:** After addressing harms, it is safe and beneficial to children's enjoyment of their rights to expand access to the online world – to more children, to children with specific accessibility needs, and to all groups of children equally.
- c) **Building a chain of responsibility and collaboration:** To continually protect and support children online, an ongoing responsibility should be placed upon the appropriate body to manage continuing efforts across relevant stakeholders.
- d) **Integrating child-centred design:** After developing policy to make the existing digital environment safer and more supportive, efforts can turn to future-proofing the regulation of the digital environment to require that children's rights and needs be considered in the development of online services.
- e) **Ensuring effectiveness:** Finally, there must be continued review of the policy to ensure it is both working as intended and responding to new and developing concerns for children in the online world.

## IV. POLICY GOALS

Taking children's rights and cross cutting issues on board, the African Union's Child Online Safety and Empowerment Policy establishes the following goals across ten policy action areas:

1. **Institutional capacity:** To identify and mobilise the institutional actors (at continental, regional and national levels) to lead and contribute to a Child Online Safety Steering Committee and a stakeholder group of experts to cover all areas of the child online safety policy. To provide adequate resourcing, leadership, and institutional capacity to ensure effective action and cooperation.
2. **Legal and regulatory frameworks:** To strengthen and re-align the continental, regional and national legal and regulatory regimes related to child online safety, and to strengthen the capacity and capability of law enforcement agencies and regulatory bodies in the child online safety field including their capacity to collaborate with other sectors, in particular the ICT sector.
3. **Personal data and identity:** To recognise the benefits of and respond to the current and emerging threats to privacy, identity and the agency of children in the digital world posed by the use of data including personal data, biometrics and automated decision making.
4. **Response and support systems:** To establish a coordinated multi-stakeholder framework to tackle risks for children online, in particular child exploitation and abuse (CSEA): including effective legal and regulatory enforcement mechanisms, prevention, remedies and access to expert advice on child online safety.
5. **Business and children's rights:** To promote child-centred design, minimum standards, industry agreements, adoption of best practice and cultural awareness and resourcing of child online safety through regulation and frameworks that relate to corporate responsibility.
6. **Training:** To ensure that all those involved with services relating to children, including government, law enforcement, justice, health and wellbeing, politicians, and civil servants, as well as those designing technology, have a good understanding of child online safety and children's best interests.
7. **Education:** To promote the positive use of digital technology as a source of entertainment, information and learning for children in a safe environment.



8. **Public awareness and communications:** To raise awareness of all child online safety issues across all sectors of the community, in order to prevent likely harms and promote positive internet use.
9. **Research and development:** To ensure a holistic, evidence-based and up to date approach to child online safety.
10. **International cooperation:** To ensure strong collaboration between stakeholders, at the continental level, as well as with other external national, regional, and global organisations and players to share best practice.

## V. IMPLEMENTATION PLAN

The following Implementation Plan sets out practical actions to advance towards the above goals. It includes actions to be implemented at the level of the African Union, as well as a framework for regional and national policy makers to design and deliver coordinated and effective mechanisms that are relevant in their specific context.<sup>35</sup> The Implementation Plan should be seen as complementary to efforts to enhance access to data and devices for children and those who support children's online safety and empowerment.

Delivery on the Implementation Plan will be coordinated by a newly established African Union Child Online Safety Steering Committee, which will also be charged with regularly reviewing and updating the Plan, in order to adapt to learnings within the context of its implementation and evolving international best practice.

For each of the action areas, the African Union Commission will assess gaps and develop recommendations to be taken forward as part of the implementation plan for this policy or put to the African Commission for further action; and develop, share and maintain a database of best practices and resources. For the development of tools and resources, care will be taken to consider existing assets from national, international or multilateral environments that can be refocused on the African context.

To ensure efficient and smooth implementation of the key actions contained in the Implementation Plan, the African Union Commission shall collaborate / coordinate with relevant African and regional institutions / organizations / partners to implement the various aspects of the Action Plan.

Goal #	Governance	
1	Affirm public commitment to child online safety at the highest level	Ministerial Declaration & High-Level launch event for the AU Child Online Safety & Empowerment Policy [2023]
1	Establish African Union Child Online Safety & Empowerment Steering / Oversight Committee	The African Union Child Online Safety & Empowerment Steering/Oversight Committee will be responsible for coordinating the implementation and review of the AU Child Online Safety & Empowerment Policy, and will serve as a focal point for regional and international cooperation. The Steering/ Oversight Committee will bring together designated Regional and National COS focal points and representatives of the AU authorities responsible for the following policy areas: education, health, justice, consumer protection, ICT, data protection, cybersecurity, law enforcement, family and children's services. It will include a selection of African and international experts that between them cover the ten

<sup>35</sup> Tools for the elaboration of more detailed and tailored regional or national policies can be found in the Child Online Safety Toolkit: <https://childonlinesafetytoolkit.org>

		policy areas, plus children's rights and the cross cutting issues. It will meet at least quarterly. The AU Secretariat will provide the secretariat for the Steering Committee.
1, 9	Establish African Union Child Online Safety & Empowerment Stakeholder Group or groups	The Child Online Safety & Empowerment Stakeholder Group will provide expertise and implementation support to the steering Committee. It will be made up of professionals and experts, including enforcement professionals, business, third sector, children's rights organisations, educational institutions, parents/carers and academia. It will include a core group of Stakeholders as well as stakeholders invited to participate for a given policy area. Its consultative function can be complemented by open calls for evidence. Child participation should be ensured across all activities. This group is intended to be an expert resource for the Steering Committee, not a second steering group with decision making powers.
1	Define performance indicators and evaluation	The inaugural in-person meeting of the African Union Child Online Safety & Empowerment Steering Committee will agree a process for the implementation of this Plan (including prioritisation and resourcing of activities), Key Performance Indicators, evaluation mechanisms, reporting structures and review mechanisms for this Plan and Policy as a whole. The Steering Committee will designate an Accountable Authority (person, institution, body) for each action in this Plan and allocate the necessary human and financial resources to successfully complete the task envisioned.
<b>Goal #</b>	<b>Legal frameworks</b>	
2, 3, 4, 5	Develop a harmonized legal framework for children's online privacy and safety by design and default, and enforcement mechanisms	The African Union Commission shall assess gaps in the current legal and regulatory regime for African children against international best practice and develop a harmonised legal framework for the protection of children's privacy and safety online grounded in children's rights and the African Charter on the Rights and Welfare of the Child. This legal framework will set out: (1) strong protections for children's data, and (2) an outcomes-based safety-by-design regime. It will cover all digital products and services likely to be accessed by children and ensure a high level of protection of children's data by design and default through age-appropriate design, including by requiring businesses to implement age assurance (if necessary), conduct risk assessments covering the 4 Cs, adhere to the highest available international standards and codes of practice and be transparent, including by providing access to data for researchers. Enforcement should be ensured by (an) independent supervisory authority/ies, with sufficient resources for the required task.
2, 4	Strengthen criminal justice frameworks to effectively tackle child online safety-related offences, including CSEA	The African Union Commission shall aspire to provide guidance on how criminal laws and procedures relating to child online safety (including the investigation, prosecution and sentencing of online offences that violate children's rights or impair their physical, mental or moral development) can be harmonised and strengthened in line with international standards and best practices. Criminal laws concerning child online safety should be developed in light of all children's rights, including their rights to be heard and to participation, and should ensure the protection of children who themselves come into conflict with the law. Criminal justice systems should ensure timely access to justice, including through effective support and reporting mechanisms for victims, and adequate resourcing of investigation and response services.
2, 4, 5, 7	Develop and implement a harmonized age-rating classification	The African Union shall encourage the development and adoption of a harmonized age-rating classification for commercial content, public service media and games and activities online that reflects the evolving capacities of children.
2, 10	Consider participation in international legal frameworks for child online safety	The African Union Commission shall assess gaps in regional and international participation of existing instruments that promote child online safety, and present recommendations to all Member States.

Goal #	Capacity-building, training and pooling of resources	
2, 3, 4, 5, 6, 10	Strengthen the capacity of regulators for the oversight and enforcement of child online privacy and safety legal frameworks	<p>The African Union Commission shall promote exchange of best practice, develop recommendations for capacity-building, develop and roll-out a training module for ICT regulators covering:</p> <ul style="list-style-type: none"> <li>(3) Children's rights in the digital environment (drawing on the UNCRC General comment No. 25 and resources developed by e.g. the ITU)</li> <li>(4) Data Privacy</li> <li>(5) Safety by design (covering the existing standards, processes and tools that support implementation and enforcement)</li> <li>(6) Protections and procurement standards for ed tech and technology used in schools</li> <li>(7) AI Oversight (based on the four-step model of children's rights respecting AI oversight)</li> </ul>
2, 4, 6, 10	Strengthen the capacity of law enforcement and criminal justice agencies	<p>The African Union Commission shall promote exchange of best practice, develop recommendations for capacity-building, develop training materials and roll-out targeted Train the Trainers programmes for law enforcement and other criminal justice practitioners for child online safety covering:</p> <ul style="list-style-type: none"> <li>(1) Privacy and data protection mechanisms</li> <li>(2) Child safeguarding and prevention of offences</li> <li>(3) How to recognise and investigate offending behaviours</li> <li>(4) Prosecution and sentencing</li> <li>(5) Offender management</li> <li>(6) Victim support</li> </ul>
4, 6, 7, 8, 10	Strengthen the capacity of professionals working directly with children	<p>The African Union Commission shall promote exchange of best practice, develop recommendations for capacity-building, develop training materials (and educational courses for relevant degree programmes) and roll-out targeted Train the Trainers programmes for professionals and volunteers who work with children in settings including education, health and social services, covering:</p> <ul style="list-style-type: none"> <li>(1) How child online safety relates to their particular role</li> <li>(2) How to develop and implement a child online safety policy in a given setting</li> <li>(3) How to support vulnerable children</li> <li>(4) How to recognise and understand offending behaviour</li> <li>(5) How to report offences</li> <li>(6) How to provide access to victim support</li> </ul>
2, 3, 4, 5, 6, 9, 10	Develop and maintain databases to pool resources and information exchange	<p>The African Union Commission shall develop and maintain databases for the sharing of information, resources and best practice, including the tracking of breaches of children's rights as well as identified harms, and for cooperation on law enforcement. These databases will be renewed, reviewed and shared on a regular basis.</p>
Goal #	Awareness, education and hotlines	
3, 4, 5, 6, 7, 8, 10	Promote and support accessible digital education in schools	<p>The African Union Commission shall promote exchange of best practice and develop education materials and an education programme to promote child online safety and empowerment in schools. The programme, which should be modifiable to local circumstances and introduced as part of the standard school curriculum, should aim to help children develop digital skills and empower them to build respectful communities. It should be holistic and cover data and media literacy, alongside safeguarding issues. It should promote the positive use of digital technology, sexuality and consent, and will consider the needs of all children, regardless of gender, age, income or background.</p>

4, 5, 6, 7, 8	Promote and support education for parents, carers and community leaders	The African Union Commission shall promote exchange of best practice and develop education materials and programmes for exchanges and awareness - raising among parents, carers and community leaders working directly with or responsible for child online safety and empowerment. Consultations with families and children are needed to identify issues, solutions and ways of raising awareness of child online safety in an effective way in the community.
7, 8	Develop and maintain a child-friendly public portal for online safety	The African Union Commission shall promote the creation of a child-friendly and accessible public portal for online safety and digital engagement, covering the full range of child online safety issues as set out in this policy. Targeted messages and materials should be designed in consultation with children, young people and parents/carers.
7, 8	Public awareness campaign around Africa Safer Internet Day	The African Union Commission shall coordinate (including with the ITU) a public awareness campaign around the issues set out in this policy on the occasion of Africa Safer Internet Day.
2, 4, 10	Support and promote hotlines for reporting and victim support	The African Union Commission shall promote exchange of best practice (including with One Stop Centres), develop recommendations for capacity-building and support the set up and promotion of comprehensive hotline structures (online and telephone) for incident reporting and victim support. These hotlines will be fully resourced and volunteers receive adequate training. It is the intention to build on the knowledge and practice of existing hotlines operating in other jurisdictions and to make bilateral 'twinning' agreements that ensure initial and ongoing support across jurisdictions.
5, 6	Promote industry best practice for COS	The African Union Commission shall promote awareness of ICT industry professionals of children's rights and the issues covered by this policy, best practices and tools for compliance. The Commission shall encourage the promotion and sharing of COS best practices by African Member States
Goal #	<b>Research</b>	
9, 10	Establish an African COS research fund and programme	The African Union Commission shall establish a central research fund and develop a research programme to provide the data and evidence necessary for the implementation and updating of this policy. The programme will support research and data collection at the national, regional and continental level to support monitoring and evaluation of child online safety measures. It will promote high research standards, the establishment of national centres of excellence, sharing of data and resources and cooperation between researchers, including at the international level. Initial and regular gap analysis will help to ensure resources are prioritised in areas of biggest need and to avoid unnecessary duplication. The resources from this fund should also focus on ensuring African Union Member States benefit from the research programmes of multilateral, regional and other states – including by supporting the engagement of domestic research programmes with colleagues and programmes across the globe.
9, 10	Develop and maintain research database	The African Union Commission shall develop and maintain a central repository for child online safety research. This database will include all research conducted under the African COS research programme as well as provide a portal for researchers to access relevant international academic work in this area. It will also promote the sharing of best practice in COS innovation, responsible research, resources and cooperation among African researchers. This research base will also act as a resource for international researchers in order that the African perspective is kept in mind.



