Child Online Protection Guidelines
Women's Health and Education Center (WHEC) Campaign
Keeping children safe in the digital environment

POLICY BRIEF

The explosion of information and communication technology (ICT) has created unprecedented opportunities for children and young people to know their rights. More and more children are connecting for the first time every day, either on personal or shared devices. However, wider and more easily available access to the Internet and digital technology also poses significant challenges to meaningful connectivity and children's rights, including their safety. Impacts range from threats to protection of personal data and privacy, to harassment and cyberbullying, harmful online content, grooming for sexual purposes, and sexual purposes, and sexual abuse and exploitation.

Child Online Protection (COP), is a global challenge, and it requires a holistic approach and a global response, international cooperation, and national coordination to protect children from online risks and potential harm and empower them to fully benefit from online opportunities.

The **Council Working Group on Child Online Protection,** has defined COP actions which include awareness of child online safety issues and assisting and supporting Member States of the United Nations (UN), in developing and implementing roadmaps for COP initiatives.

The global challenge of COP requires a global response, international cooperation, and national cooperation. With more reliance on digital technologies, risks for children online and stresses the urgent need for action. The challenges and threats persist due to the borderless nature of the online environment among other reasons that hinder the protection of children through a lack of dedicated international and national legislative frameworks, plans, strategies, resources including funding, and institutions to ensure child online protection. This has created unprecedented opportunities for children and young people to communicate, learn, socialize, and play, exposing them to new ideas and more diverse sources of information.

Young people are the driving force of connectivity globally, with 75% of 15 to 24 years-olds online in 2022, compared with 65% for the rest of the world's population. Children are also spending more time online than ever before. And they are getting there sooner. Around the world, a child goes online for the first time every half second! According to UNICEF (2020) – at the global level, 1 in 3 Internet users is a child under 18 years of age. Over a billion and a half children were affected by the closure of educational institutions at the peak of the COVID-19 crisis in 2020. COP therefore seeks to reduce risks and protect children from harms they may encounter online. These include:

1. **Content Risks.** Exposure to inaccurate or incomplete information, inappropriate or even criminal content such as exposure to adult/extremist/violent/gory content, self-abuse and

self-arm related content, destructive and violent behavior, radicalization or subscribing to racist or discriminatory ideas;

2. **Contact Risks from Adults or Peers.** Harassment, exclusion, discrimination, defamation and damage to reputation, and sexual abuse and exploitation including extortion, grooming (sexual), child sexual abuse material, trafficking and sexual exploitation of children in travel and tourism as well as extremist recruitment;

3. **Contract Risks:** Exposure to inappropriate contractual relationships, children's consent online, embedded marketing, online gambling, as well as violation and misuse of personal data such as hacking, fraud and identity theft, scams profiling bias;

4. **Conduct Risks:** Such as sharing of self-generated sexual content or risks characterized through hostile and violent peer activity such as cyberbullying, stalking, exclusion and harassment.

Risks & Cyberbullying: Developing a National Strategy

Cyberbullying and other forms of peer-to-peer violence can affect young people each time they log in to social media or instant messaging platforms. Over a third of young people in 30 countries report being cyberbullied, with 1 in 5 skipping school because of it. When browsing the Internet, children and young people may be exposed to hate speech and violent content – including messages that incite self-harm and even suicide. Young internet users are also vulnerable to recruitment by extremists and terrorist groups. Digital platforms have also been used as vectors for disinformation and conspiracy theories that have a harmful effect on children and young people. Most alarming is the threat of online *Sexual Exploitation* and abuse. Some 80% of children in 25 countries report feeling in danger of sexual abuse or exploitation online.

A national COP strategy provides the roadmap to bring together and coordinate existing and new activities relevant for child (online) protection. Any strategy should be owned by a suitable authority and be sustainable with the required human and financial resources. Such a framework should have a clear mandate and sufficient authority through a multi-stakeholder mechanism (or council) to coordinate all activities related to children's rights and digital media and ICTs at cross-sectoral, national, regional and local levels, appreciating existing efforts in the definition, coordination, implementation and monitoring of the national COP strategy.

Women's Health and Education Center 's Proposed Guidelines for Child Online Protection (COP)

The multistakeholder approach for the development of global platform and network of any kind of guidance related to digital ecosystem is the overall strategy of *Women's Health and Education Center (WHEC)*. The focus of the Guidelines on challenges related to WHEC's work in the areas of Education, the Sciences, and Culture. The aim of Guidelines is to safeguard freedom of expression, access to information, and other human rights in the context of the development and implementation of digital platform regulatory processes.

Child Online Protection (COP) is a global challenge. Due to the rapid advancements in technology and society, and the borderless nature of the Internet, child online protection need to be agile and adaptive to be effective. Overarching Principles are:

1. Be based on a holistic vision that incorporates government, industry, and society, ensuring relevant multi-social action and accountability.
2. Be set at the highest level of government, which will be responsible for assigning relevant roles and responsibilities and allocating sufficient human and financial resources.
3. Result from and all-encompassing evidence-based understanding of the digital environment yet be tailored to national priorities.
4. Respect and be consistent with the fundamental rights and freedoms of children as enshrined int the UN Convention on the Rights of the Child and other key international conventions and laws.
5. Respect, be consistent with and build upon existing, similar, and related domestic laws and strategies in place.
6. Be developed with the active participation of all relevant stakeholders including children and their families, addressing their needs and responsibilities, and meeting the needs of vulnerable groups.
7. Be designed to align with broader government plans for economic and social development, including investment and resource mobilization to child online protection efforts.
8. Utilize the most appropriate policy instruments available to realize its obligative.
9. Guide efforts of stakeholders to empower and educate children, carers, and educators as digital citizens including digital access, equity and digital literacy.
10. Contribute to the development of a trusted digital environment that is safe for children

An inclusive, multifaceted child online protection strategy with effective and targeted measures and activities including financial and human resources to implement the strategy is necessary at all levels. Only with a coordinated and cooperative multi-stakeholder approach will children and future generation be protected and empowered to thrive in digital environments.

POLICY ACTIONS

The following policy actions aim to addressing all risks and potential harms for children online and are meant to be complimented by more specific frameworks.

Child Rights

Standardize the definition of a child as anyone under the age of 18 in all legal documents in line with Article 1 of the United Nations Convention on the Rights of the Child (UN CRC). Build on and collaborate with independent human rights institutions for children to ensure children's protection online through specialized expertise, investigation and monitoring, promotion, awareness raising, training and education, and with children's participation.

Legislation

Review the existing legal framework to determine that all necessary legal powers exist to enable and assist law enforcement and other relevant actors to protect persons under the age of 18 from

all types of online harms on all online platforms. Encourage the use of appropriate terminology in the development of legislation and policies addressing the prevention and protection of sexual exploitation and sexual abuse of children. **Child sexual abuse material (CSAM)** – Legislation must exist in all UN Member States, that makes it a criminal offence to download, access, view, store, possess, distribute, display, or exhibit and make available any sexual content depicting and featuring children under 18 years of age for primarily sexual purposes.

Law Enforcement

Ensure that cases of children who harm others online are dealt with in line with child rights principles, appropriately inscribed in national legislation, strongly favoring tools other than the criminal law. Provide appropriate financial and human resources, as well as training and capacity building to fully engage and equip the law enforcement community. Ensure international cooperation between law enforcement agencies around the world, allowing a quicker response to online-facilitated crimes.

Regulation

Consider the development of a regulatory policy. Place an obligation on businesses to undertake child-rights due diligence and to safeguard their users. Establish monitoring mechanisms for the investigation and redress of children's rights violations, with a view to improving accountability of ICT and other relevant companies. Strengthen regulatory agency responsibility for the development of standards relevant to children's rights and ICTs.

Monitoring and Evaluation

Establish a multi-stakeholder platform to steer the development, implementation, and monitoring of the national digital agenda for children. Develop time bound goals and a transparent process to evaluate and monitor progress and ensure that the necessary human, technical, and financial resources are made available for the effective operation of the national COP strategy and related elements.

Information Communication Technology (ICT) Industry

Ensure that ICT industry uses rigorous mechanisms to detect, block, remove, and proactively report illegal content and any abuse (classified as criminal activity) against children. Encourage ICT industry to adopt a safety and privacy by design approach to their products, services and platforms, recognizing respect for children's rights as a core objective. Support ICT industry stakeholders to provide age-appropriate family friendly tools to help their users to better manage the protection of their families online.

Reporting

Establish and widely promote mechanisms to easily report illegal content found on the Internet. Establish a national child helpline with the necessary capacity on online facilitated risks and harms or child online safety concerns by victims. Establish safe and accessible child-sensitive counseling, reporting, and complaint mechanisms.

Social Services and Victim Support

Ensure that universal and systematic child protection mechanisms are in place that oblige all those working with children (e.g., social care, healthcare professionals, educators) to identify, respond to and report any sort of harm to children that occurs online. Ensure social services professionals are trained both for preventive action and response to online harms to children, identifying child abuse and providing adequate specialized and long-term support and assistance for child victims of abuse.

Develop child abuse strategies and measures based on scientific evidence. Provide appropriate human and financial resources to ensure the full recovery and reintegration of children and to prevent revictimization of child victims. Ensure that children have access to adequate health care (including mental health as well as physical well-being), including in the event of victimization, trauma, or abuse online.

Data Collection and Research

Invest in and align the development, monitoring and evaluation of frameworks and activities. Undertake research of the spectrum of national actors and stakeholders to determine their opinions, experiences, concerns and opportunities with regard to COP.

Education

Ensure educators and school administrators/professionals are trained to identify and adequately respond in suspected or confirmed cases of child victims of abuse. Develop a broad digital literacy program that is age-appropriate and focused on skills and competencies to ensure that children can fully benefit from the online environment, are equipped to identify threats, and can fully understand the implications of their behavior online. Such a program can be built upon existing educational frameworks.

Develop digital literacy features as part of the national school curriculum that is age-appropriate and applicable to children from an early age. Create educational resources outside the school curriculum that emphasize the positive and empowering aspects of the Internet for children and promote responsible forms of online behavior. <u>Avoid fear-based messaging</u>. Consult children, as well as parents and carers on the development of educational programmes, tools, and resources.

National Awareness and Capacity

Develop national public awareness campaigns, covering a wide variety of issues that can be linked to the digital environment and tailored to all target groups. Enlist pubic institutions and mass media for the promotion of national public awareness campaigns. Harness global campaigns, as well as multi-stakeholder frameworks and initiatives to build national campaigns and strengthen national capacities on COP.

Resources

1. United Nations Human Rights; Office of the High Commissioner
UN Document: CRC/C/GC/25
Children's Rights in Relation to the Digital Environment
https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

2. UNICEF (2020)
Protecting Children Online
https://www.unicef.org/protection/violence-against-children-online

3. UNICEF
Cyberbullying: What is it and How to stop it?
https://www.unicef.org/end-violence/how-to-stop-cyberbullying

4. ITU (International Telecommunication Union) COP Implementation
Child Online Protection Guidelines and Implementation
https://www.itu-cop-guidelines.com/implementation

5. Women's Health and Education Center (WHEC)
WHEC Global Health Line (WGHL)
http://www.womenshealthsection.com/content/cme/WHEC_Global_Health_Line.pdf

   LINK Access Project
   http://www.womenshealthsection.com/content/documents/LINK-Access-Project.pdf