Policy brief

Keeping children safe in the digital environment: The importance of protection and empowerment

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 abuse and exploitation.

The global challenge of child online protection (COP) requires a global response, international cooperation, and national coordination. With more reliance on digital technologies, the COVID-19 pandemic aggravates previously existing 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.[1]

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 generations be protected and empowered to thrive in digital environments.

1 UNICEF. 2020. Action to End Child Sexual Abuse and Exploitation: A Review of the Evidence 2020

With 69 per cent of young people online in 2019,[1] and one in three children with Internet access at home, the Internet has become an integral part of children's lives, presenting many possibilities for children and young people to communicate, learn, socialize and play, exposing children to new ideas and more diverse sources of information, opening opportunities for political and civic participation for children to thrive, be creative, and meaningfully contribute to a better society.[2]

With more than 1 billion children away from their school building and learning remotely in 2020 and into 2021, the COVID-19 pandemic has underlined the importance of meaningful connectivity as (in many cases) the viable means for access to basic education, social interactions, and access to help and support services. Accessible and affordable connectivity is increasingly a determinant of equal opportunity for children in particular for those who are left behind in current systems – whether because of poverty, disability, race, ethnicity, gender, displacement or geographic isolation. ICTs can help them fulfil their educational potential, facilitate their social inclusion, and amplify their voices in civic participation – pursuant to their rights under the United Nations Convention on the Rights of the Child (UN CRC).

At the global level, one-in-three Internet users is a child under 18 years of age.

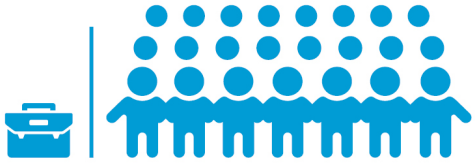
1 ITU. 2020. Measuring digital development: Facts and figures

2 UNICEF. 2020. Digital civic engagement by young people
UNICEF. 2020. Pandemic participation: youth activism online in the COVID-19 crisis
Office of the Special Representative of the Secretary-General on Violence against Children. 2021. Children as agents of positive change

While supporting and promoting children's rights, the same online environment may expose children to risks, some of which can translate into potential harms.[3] In April 2020 alone, the National Center for Missing and Exploited Children (NCMEC) registered four million reports of suspected child sexual abuse material (CSAM) online, compared to one million for the same period in 2019.[4]

Child online protection therefore seeks to reduce risks and protect children from harms they may encounter online. These include[5]:

- 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-harm related content, destructive and violent behaviour, radicalization or subscribing to racist or discriminatory ideas;
- 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;
- 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;
- 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.



Over 1.5 billion children have not attended lessons at school due to COVID-19

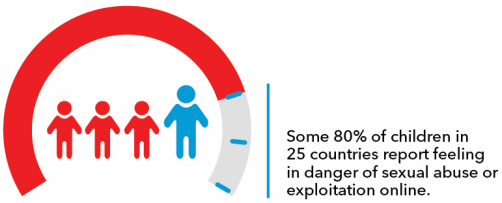
At the global level, one-in-three Internet users is a child under 18 years of age.

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.

More than a third of young people in 30 countries report being cyberbullied, with 1-in-5 skipping school because of it. Some 80 per cent of children in 25 countries report feeling in danger of sexual abuse or exploitation online.[1]

In 2020, NCMEC CyberTipline received 21.7 million reports of suspected CSAM, an increase of 28 per cent from 2019.

[1] UNICEF. 2020. Protecting children online



The UN CRC recognizes that children are an especially vulnerable group and upholds children's rights including among others the right to protection from all forms of exploitation, the right to privacy, freedom of expression or the right to participation, all in the context of the principle of evolving capacities. These rights also apply in the digital environment as per the principles set by the UN CRC General Comment No. 25 (2021) on children's rights in relation to the digital environment.[6] Protecting children and young people is a shared responsibility and policy-makers, industry, parents, carers, educators, and other stakeholders must ensure a sustainable future where children and young people can thrive and fulfil their potential – online and offline – and where they can be guaranteed a safe-by-design and empowering digital environment.[7]

[3] Global Partnership to End Violence against Children and partners (ITU, UNESCO, UNICEF, UNODC, WePROTECT Global Alliance and World Childhood Foundation USA). 2020. Technical note: COVID-19 and its implications for protecting children online

[4] NCMEC. 2020. CyberTipline 2020: Rise in Online Enticement and Other Trends From Exploitation Stats

[5] Livingstone and Stoilova. 2021. The 4Cs: Classifying Online Risk to Children.
OECD. 2021. Children in the digital environment: Revised Typology Of Risks

[6] UN OHCHR. 2021. General Comment No. 25 (2021) on children's rights in relation to the digital environment. www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

[7] Australian Government eSafety Commissioner. 2018. Safety by Design. https://www.esafety.gov.au/about-us/safety-by-design

A global challenge

The child population worldwide is growing and while many children are coming online for the first time, many others remain unconnected and deprived of the opportunities the Internet offers for children to learn, play, communicate and engage. The digital divide goes beyond issues of connectivity and is strongly linked to digital skills and digital literacy of children and families.

To become confident digital citizens, and to generate future generations of digital entrepreneurs, innovators and leaders of tomorrow, children must be granted not only access to the Internet but protection from online harm, and the digital citizenship skills to navigate online risks and threats. Only through such meaningful connectivity (connecting, protecting, and educating children on the online environment), and by investing in the future of society, the economy and political prosperity, can equal and safe digital transformation be achieved. Examples of efforts towards expanding connectivity among children include Giga,[8] which was launched by UNICEF and ITU in September 2019, to connect every school to the Internet and every young person to information, opportunity, and choice.

Meaningful connectivity[9] and online safety education[10] are now more vital than ever. The COVID-19 pandemic has shown the urgent need to act and strengthen meaningful connectivity to uphold children's rights, and it has put children at a higher risk of harm through that connectivity.[11] If children are spending more time online, so too are the perpetrators who groom children, search for victims or seek and share child sexual abuse material. To assist key stakeholders to take urgent measures to mitigate potential risks and ensure children's online experiences are safe and positive during COVID-19, the Global Partnership to End Violence against Children, together with its partners (ITU, UNESCO, UNICEF, UNODC, WePROTECT Global Alliance, WHO, and World Childhood Foundation USA) released a technical note and a resource pack.[12]

Evidence shows that children who are more vulnerable online are often more vulnerable offline, and that protective offline factors can also reduce exposure to online risks.[13] Vulnerable children, or those living with offline risks or disadvantage, are more exposed to online risks and, in turn, find themselves more likely to experience harm and less able to find support.

Due to the global nature of the digital environment, international cooperation is needed to develop an effective response. However, the lack of harmonized laws in line with international human rights standards (such as the UN CRC and its optional protocols) and international cooperation and inadequate dedicated investment remain key challenges for the protection of children online. This international dimension and the need for further trans-national cooperation have become even more evident with the authoritative guidance of the UN CRC General Comment No. 25 (2021) on children's rights in relation to the digital environment,[14] which not only states how digital technologies affect the full range of children's rights in positive and negative ways but furthermore calls for international harmonization on this issue. The General Comment targets key stakeholders to acknowledge the importance of child rights considerations in the digital environment and reaffirms the foundational principles of children's rights on the Internet. It calls for greater action and institutional capacity in situations of violence and abuse against children, and for greater responsibilities of States and businesses to provide a safe-by-design digital environment for children.

At the national level, few relevant stakeholders are sufficiently engaged, children and their parents, carers and guardians are rarely consulted, and the private sector impacts and responsibilities towards children's rights are often overlooked. Online safety prevention and response mechanisms are seldom included in child protection system and violence against children (VAC) prevention agenda, and the complexity of the risk and protective factors, and interlinkages between offline and online VAC are rarely recognized and fully understood. With little likelihood of harmonized activities on child online protection, there is often a challenge in coordinating efforts that are few and far between. Challenges remain in the development of necessary national policy frameworks with regard to safety-by-design of digital platforms, digital literacy and broad societal awareness of child online protection issues. Without filling these gaps, the transition towards an inclusive digital environment and therewith economic and social inclusion will remain hard to achieve, bringing further consequences for national economies and beyond.

At the design and solutions development level, there is also an opportunity to bring industry and child participation together. Examples of these efforts are, among others, the Safe Online portfolio and the Technology Coalition Research Fund implemented by the Global Partnership to End Violence against Children,[15] the ITU COP Guidelines for industry (2020), the ITU Youth survey undertaken by Youth and Media, Berkman Klein

[8] Giga Connect. 2019. https://gigaconnect.org/

[9] Meaningful connectivity here is understood as a framework to track the components of connectivity that matter most to users and help decision makers adopt the policies needed to connect people to an Internet that is useful and empowering.

[10] An overview of existing educational frameworks can be found at Cortesi, Sandra, Alexa Hasse, Andres Lombana-Bermudez, Sonia Kim, and Urs Gasser. 2020. Youth and Digital Citizenship+ (Plus): Understanding Skills for a Digital World. Berkman Klein Center for Internet & Society

[11] Lobe, B., Velicu, A., Staksrud, E., Chaudron, S. and Di Gioia, R. 2020. How children (10-18) experienced online risks during the Covid-19 lockdown

[12] Global Partnership to End Violence against Children and Partners. 2020. Resource Pack: COVID-19 and its implications for protecting children online

[13] UNICEF. 2021. Investigating Risks and Opportunities for Children in a Digital World

[14] More about the General Comment including a terminology glossary, explanatory note and child-friendly version, can be found at OHCHR | GC children's rights in relation to the digital environment

[15] Global Partnership to End Violence against Children. 2021. The Safe Online Portfolio and The Tech Coalition Safe Online Research Fund

Child online protection is a global challenge.

Due to the rapid advancements in technology and society, and the borderless nature of the Internet, child online protection needs to be agile and adaptive to be effective.

Child online protection requires a holistic strategy to build safe, gender-sensitive, age-appropriate, inclusive, and rights respecting digital environments for children and young people that is characterized by:

- a child rights-based approach, upholding the rights and responsibilities of society to respect children's rights as enshrined in the UN CRC and in General Comment No. 25 (2021) on children's rights in relation to the digital environment;[1]
- a dynamic balance between ensuring protection and providing equal and safe opportunity for children to be digital citizens;
- prevention of all harms;
- child-centred response, support, and self-help in the face of threats, with specific reference to the COVID-19 crisis and the response and recovery scenarios in that regard.

This approach shall also incorporate child participation in the design, implementation, and evaluation of the solutions to keep children safe online.

[1] UN OHCHR. 2021. General comment No. 25 (2021) on children's rights in relation to the digital environment. www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

Center for Internet & Society, Harvard University,[16] UNICEF tools and guidance for industry on incorporating child rights considerations[17] or the revised Safety by Design[18] (eSafety Commissioner of Australia 2018) or Risky-by-Design[19] (5Rights Foundation 2021) initiatives, which put children's rights and safety at the centre of the design, development, and release of online products and services.

Developing a national strategy

In order to effectively respond to online risks and harms for children, an inclusive multi-stakeholder national child online protection strategy includes the development of new policies (and integrates and references existing policies) and will provide the necessary framework to the global challenge of child online protection.[20] The strategy should be fully integrated with policy frameworks relevant to children's rights and complement national child protection policies by offering a specific framework for all risks and potential harms for children that aims to ensure a safe, inclusive, and empowering digital environment.

Such a strategy strengthens effective coordination among stakeholders and should consider the importance, articulate the vision, and define the role of the following stakeholders:

- government ministries at local, national and regional levels (e.g. internal affairs, health, education, justice, social welfare/child protection, digital / information, regulators);
- law enforcement;
- social and health care service organizations (e.g. counselling, support services, youth welfare office, safe houses, rehabilitation, health care services);
- ICT industry - e.g. online platforms, content providers, Internet service providers (ISPs) and other electronic service providers (ESPs), mobile phone network providers, public Wi-Fi providers;
- International organisations, NGOs, CSOs and community-based organisations (e.g., child protection and other relevant International organisations and NGOs, teacher/parent unions and organizations);
- children and young people, as well as their parents, guardians and carers;
- academic and research community (e.g. think-tanks, research centres, libraries, schools and universities).

A national child online protection 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 child online protection strategy.

[16] ITU Generation Connect. Youth and Media, Berkman Klein Center for Internet & Society, Harvard University. 2020., ITU Generation Connect. 2020 Youth Engagement Survey and Data and Interpretation
[17] UNICEF. 2021. https://sites.unicef.org/csr/ict_tools.html
[18] Australian e-Safety Commissioner. 2018. Safety by Design Initiative
[19] 5Rights Foundation. 2021. Risky-by-Design Initiative
[20] Existing examples of relevant frameworks: With respect to child online sexual exploitation and abuse: WePROTECT Global Alliance. 2016. WePROTECT Model National Response and 2019. Global Strategic Response framework. With respect to violence against children: World Health Organization. 2016. INSPIRE framework

Overarching principles

A forward-looking and holistic national child online protection strategy including the relevant policies and enforcement/accountability mechanisms, should be developed considering ten cross-cutting principles:

1. Be based on a holistic vision that incorporates government, industry, and society, ensuring multi-sectoral 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 an 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 in 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 objective.
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.

Policy actions

The following policy actions aim at addressing all risks and potential harms for children online and are meant to be complemented by more specific frameworks such as the WePROTECT Model National Response (MNR) on child sexual exploitation and abuse, which focus on specific harms.

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.
- Include direct consultation with children as is their right under Article 12 of the UN CRC, into the development, implementation, and monitoring of any kind of child online protection framework or action plan.

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.
- Establish that any illegal act against a child in the real world is, *mutatis mutandis*, illegal online and that the online data protection and privacy rules for children are adequate.
- Align legal frameworks with existing international standards, laws, and conventions related to children's rights and cybersecurity, facilitating international cooperation through the harmonization of laws.
- 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 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.

Align national legislation with existing frameworks such as the 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 (2019) of the Committee of the Rights of the Child, the ICMEC CSAM Model Legislation & Global Review (2018), or the INSPIRE framework indicator guidance and results framework on legislation on sexual abuse and exploitation (2018).

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 favouring 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 (co-regulatory policy development, full regulatory framework).
- 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 child online protection strategy and related elements.

ICT industry

- Engage industry in the process of elaborating child online protection laws and common metrics to measure all relevant aspects of child online safety.
- Establish incentives and remove legal barriers to facilitate the development of common standards and technologies to combat content risks for children.
- Encourage 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.
- Ensure that industry uses rigorous mechanisms to detect, block, remove, and proactively report illegal content and any abuse (classified as criminal activity) against children.
- Ensure that industry provides suitable and child-friendly reporting mechanisms for their users to report issues and concerns and where users can obtain further support.
- Collaborate with industry stakeholders to promote awareness in order to support industry to identify hazards in development and correct existing products and services. This includes considering other stakeholder concerns and the risks and harms to which the end users are being exposed.
- Support 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 hotline/child helpline to facilitate reporting of child online safety concerns by victims.
- Establish safe and easily accessible child-sensitive counselling, 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 preventative 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 prevention 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 child online protection.

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 programme 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 behaviour online. Such a

programme 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 behaviour.
- Avoid fear-based messaging.
- 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 public institutions and mass media for the promotion of national public awareness campaigns.
- Harness global campaigns, as well as multistakeholder frameworks and initiatives to build national campaigns and strengthen national capacities on child online protection.

References

Global Partnership to End Violence against Children and partners (ITU, UNESCO, UNICEF, UNODC, WePROTECT Global Alliance and World Childhood Foundation USA), Technical note: COVID-19 and its implications for protecting children online, 2020.

Global Partnership to End Violence against Children and partners (ITU, UNESCO, UNICEF, UNODC, WePROTECT Global Alliance and World Childhood Foundation USA), Resource pack: COVID-19 and its implications for protecting children online, 2020.

European Council. 2020. One in five children suffers one or another form of sexual abuse or victimisation during their childhood.

Livingstone and Stoilova. 2021. The 4Cs: Classifying Online Risk to Children

Office of the Special Representative of the Secretary General on Violence against Children. 2021. Children as agents of positive change

ITU. 2020. Guidelines for policy-makers on Child Online Protection

ITU. 2020. Guidelines for industry on Child Online Protection

ITU. 2020. Guidelines for parents and educators on Child Online Protection

ITU. 2020. Guidelines for children on Child Online Protection

ITU. 2020. Measuring digital development

ITU, UNESCO: Broadband Commission. 2019. Child Safety Online: Minimizing the Risk of Violence, Abuse and Exploitation Online

ITU and ILO, IOM, UNICEF, UNHCR, UNOHR, UNODC. 2020. Inter-Agency Working Group on Violence against Children Agenda for Action

UNICEF. 2021. Investigating Risks and Opportunities for Children in a Digital World

United Nations. 2020. Policy Brief: The impact of COVID-19 on children

WePROTECT Global Alliance. 2015. Working to protect children from the growing threat of sexual exploitation and abuse online

For further resources, please refer to the reference material in the ITU Guidelines for policy-makers on Child Online Protection and the additional resource list on http://www.itu-cop-guidelines.com.

In partnership with:

This policy brief was developed within the ITU Child Online Protection (COP) Initiative and draws on the series of the 2020 ITU guidelines on child online protection. Invaluable contributions were received by Youth and Media at the Berkman Klein Center, *Harvard University, Child Online Africa, the Global Partnership to End Violence against Children, The International Center for Missing and Exploited Children (ICMEC), the Joint Research Centre (JRC) of the European Commission, the Office of the Special Representative of the Secretary-General on Violence against Children, Parent Zone, TaC-Together against Cybercrime International, UNESCO, the UK Safer Internet Centres, and the WeProtect Global Alliance as well as the 5Rights Foundation.*

ITUPublications
Published in Switzerland, Geneva, 2021

International Telecommunication Union
Place des Nations, CH-1211 Geneva Switzerland