ITU Publications

International Telecommunication Union
Development sector

Guidelines for policy-makers on Child Online Protection

2020

ITU

Guidelines for policy-makers on Child Online Protection

2020

Introduction

The Internet has transformed how we live. It is entirely integrated into the lives of children and young people, making it impossible to consider the digital and physical worlds separately. One third of all Internet users today are children and young people, and UNICEF estimates that 71 per cent of young people are already online.

Digital technologies have opened up many new ways to communicate, play games, enjoy music and engage in a vast array of cultural, educational and skill-enhancing activities. The Internet can provide crucial access to health and educational services as well as information on topics that are important for young people but may be taboo in their societies.

However, just as children and young people are often at the forefront of adopting and adapting to the new connected technologies together with the opportunities and benefits they bring, they are also being exposed to a range of content, contact and conduct threats and harms online. It is important for policy-makers to appreciate these threats and harms in formulating policy responses.

Governments, the ICT industry and civil society need to work with children and young people to understand their perspectives and spark genuine public debate about risks and opportunities. Supporting children and young people to manage online risks can be effective, but governments must also ensure that there are adequate support services for those who experience harm online, and that children are aware of how to access those services.

Table of Contents

1 What is child online protection?

Child online protection (COP), is the holistic approach to respond to all potential threats and harms children and young people may encounter online. It is everyone's responsibility to protect children from these harms.
In context of child online protection, whilst most children will be susceptible in one form or another to online threats and harms, it is important to appreciate that some children are especially vulnerable, particularly migrant children or children living with a form of disability.

2 Preparation for a national child online protection strategy

In developing a national strategy to promote online safety, policy-makers should consider a range of aspects. Initially they should identify and engage with the following **stakeholders** to understand their experiences, perceptions, opinions together with their existing activities and interventions.

- Children and young people
- Parents, guardians and educators
- Government Ministries
- Industry and connectivity providers
- Research and academia
- Non-governmental organizations
- Law enforcement
- Health and Social services

It is likely, across the range of actor and stakeholders, that there are already existing **activities** and actions with the objective to protect children online, but that these have occurred in isolation. It is important to understand and appreciate existing efforts in the development of the national child online protection strategy. The strategy should look to coordinate and direct efforts through the orchestration of both existing and new activities. The strategy should be included within, or cross- reference, existing national frameworks or strategy plans.

Alongside an understanding of the activities and experiences of the various actors and stakeholders, it is essential to consider the circumstances and responses from other countries. There have been innovative developments and initiatives in the regulatory and institutional response to threats to children's safety and wellbeing online. In addition to appreciating what is possible, it also helps policy- makers to challenge existing provision and potential; and identify areas of cross-border collaboration and engagement. A number of these **national and international initiatives and developments** are signposted in these guidelines.

There are clear benefits from a national child online protection strategy. The development of adequate **national legislation**, the related **legal framework**, and within this approach, **harmonisatio**n at the international level, are keys steps in protecting children online. These frameworks may be self- regulatory, co-regulatory or full regulatory frameworks.

3 General recommendations

With an understanding of existing national activities, interventions and frameworks together with examples from other countries, policy-makers should be in a position to start to plan for the development of a national child online protection strategy. These guidelines include a series of recommendations that may be considered including the legal and policy frameworks.

These frameworks should address all harms against children in the digital environment but at the same time, this should not unduly restrict children's rights.
The frameworks should integrate and reference existing policy frameworks.
The frameworks should specifically cover the sexual exploitation of children online (including child sexual abuse material) as well as national education provision and expectations for industry providers.

It is important that the frameworks detail the objectives and to define the evaluation criteria. A multi-stakeholder mechanism should be developed that defines, coordinates and drives the national activities under the direction of the national child online protection strategy. This mechanism should be the vehicle that brings together, and orchestrates, the spectrum of national actors and stakeholders.
These guidelines highlight a series of further recommendations for policy-makers to consider in developing and starting to design a national child online protection strategy.

4 A national checklist

Area	Area for consideration
Legal framework	Review the existing legal framework to determine that all necessary legal powers exist to enable law enforcement and other relevant agencies to protect persons under the age of 18 online on all Internet-enabled platforms.
	Establish, mutatis mutandis, that any act against a child which is illegal in the real world is illegal online and that the online data protection and privacy rules for children are also adequate.
Regulatory framework	Consider the regulatory policy development. This may include a self or co-regulatory policy development as well as a full regulatory framework.
Reporting - illegal content	Ensure that a mechanism is established and is widely promoted to provide readily understood means for reporting the variety of illegal content found on the Internet.
Reporting- user concerns	Industry should provide users with the opportunity to report concerns and issues to their users and respond accordingly.
Actors and stakeholders	Engage all the relevant national stakeholders with an interest in online child protection.

Area	Area for consideration
Research	Undertake research of the spectrum of national actors and stakeholders to determine their opinions, experiences, concerns and opportunities with regards to child online protection.
Education digital literacy and competency	Develop digital literacy features as part of any national school curriculum that is age appropriate and applicable to all children.
Educational resources	Develop Internet safety messages and materials, which reflect local cultural norms and laws and ensure that these are efficiently distributed and appropriately presented to all key target audiences.
Child protection	Ensure that universal and systematic child protection mechanisms are in place that oblige all those working with children to identify, respond and report incidents of abuse and harm that occur online.
National awareness	Organise national awareness campaigns to create the opportunity to universally highlight child online pro- tection issues.
Tools, services and settings	Consider the role of device settings, technical tools (such as filtering programmes) and child protection apps and settings that can help.

General guidelines for all related industry

The guidelines outline broad recommendations for industry for identifying, preventing and mitigating any adverse impacts of products and services on children and young people's rights, and for promoting children and young people's positive use of ICTs.

A

Industry can identify, prevent and mitigate the adverse impacts of ICTs on children and young people's rights, and identify opportunities to support the advancement of children and young people's rights by taking the following actions:

- Develop a child protection and safeguarding policy and/or integrate specific risks and opportunities pertaining to children and young people's rights into company-wide policy commitments (e.g. human rights, privacy, marketing and relevant codes of conduct).
- Identify child rights impacts on different age groups as a result of company operations and the design, development and introduction of products and services, as well as opportunities to support children and young people's rights.
- Adopt an empowerment and education-based approach to child protection. Consider children's data protection rights, their right to privacy and to freedom of speech, while offering education and guidance through the company's services.
- In States which lack adequate legal frameworks for the protection of children and young people's rights to privacy and freedom of expression, companies should ensure policies and practices are in line with international standards. See United Nations **General Assembly Resolution 68/167** on the right to privacy in the digital age.

B

In collaboration with government, law enforcement, civil society and hotline organizations, indus- try has a key role to play in combating CSAM by taking the following actions:

- Prohibit uploading, posting, transmitting, sharing or making available content that violates the rights of any party or infringes any local, state, national or international law.
- Communicate with national law enforcement agencies or the national hotline(s) to communicate reports of CSAM as soon as these are brought to the provider's knowledge.
- Ensure that internal procedures are in place to comply with reporting responsibilities under local and international laws.
- Develop notice and take down and reporting processes that allow users to report CSAM or inappropriate contact and the specific profile/location where it was detected.
- Include data retention and preservation policies to support law enforcement in the event of criminal investigations through such activities as capturing evidence.
- Actively assess all content hosted on the company's servers, including commercial (branded or contracted from third-party content providers) on a regular basis. Consider using tools such as hash scanning of known child sexual abuse images, image recognition software or URL blocking to handle CSAM.

Industry can help create a safer, more enjoyable digital environment for children and young people of all ages by taking the following actions:

C

- Adopt safety and privacy-by-design principles in the company's technologies and services and prioritize solutions that reduce the volume of data relating to children to a minimum.
- Implement age-appropriate designs in the services offered.
- Present information to children regarding the rules of the site in an accessible and age- appropriate manner, providing the appropriate amount of detail.
- Consider providing mechanisms such as parental control software and other tools that enable parents and carers to manage their children's access to Internet resources while providing guidance to them on their appropriate usage so that children's rights are not infringed on. These include block/allow lists, content filters, usage monitoring, contact management and time/ programme limits.
- Avoid harmful or inappropriate advertising content online and establish customer disclosure obligations for service providers with content that is intended for an adult audience and could be harmful to children and young people.
- Ensure that data collection policies comply with relevant laws concerning children and young people's privacy, including considering whether parental consent is required before commercial enterprises can collect personal information from or about a child.
- Ensure that content and services that are not appropriate for users of all ages are:
  - classified in line with national standards and cultural norms;
  - consistent with existing standards in equivalent media;
  - identified with prominent display options to control access;
  - offered together with age verification, where possible appropriate and with clear terms relating to erasure of any personally identifiable data obtained through the verification process.
- Offer clear reporting tools and develop a follow-up process to reports of inappropriate content, contact and misuse, and provide detailed feedback to service users on the reporting process.
- Ensure pre-moderation of interactive spaces designed for children and young people in ways that are congruent with children's right to privacy and their evolving capacities.
- Promote national support services that enable children and young people to report and seek support in the case of abuse or exploitation

Industry can complement technical measures with educational and empowerment activities by taking the following actions:

D

- Educate customers on how to manage concerns relating to Internet use, including spam, data theft and inappropriate contact such as bullying and grooming, and describe what actions customers can take and how they can raise concerns on inappropriate use.

- Collaborate with government and educators to build parents' capacities to support and talk to their children and young people about being responsible digital citizens and ICT users.
- Based on the local context, provide educational materials for use in schools and homes to enhance children and young people's use of ICTs and to develop critical thinking to enable them to behave safely and responsibly when using ICT services.

Using technology advances to protect and educate children

- Privacy-preserving AI, which understands texts, images, conversations and contexts, can detect and address a range of online harms and threats, and use that information to empower and educate children to deal with them. When performed within the smart device environment, this can protect young people's data and privacy while still supporting them.

Industry can encourage and empower children and young people by supporting their right to participation through the following actions:

- Provide information about a service to highlight the benefits children obtain by behaving well and responsibly, such as using the service for creative purposes.
- Establish written procedures that ensure consistent implementation of policies and processes that protect freedom of expression for all users, including children and young people, as well as documentation of compliance with these policies.
- Avoid over-blocking of legitimate and developmentally appropriate content. In order to ensure that filtering requests and tools are not misused to restrict children and young people's access to information, ensure transparency about blocked content and establish a process for users to report inadvertent blocking.
- Develop online platforms that promote children and young people's right to express themselves; facilitate their participation in public life; and encourage their collaboration, entrepreneurship and civic participation.
- Collaborate with local civil society and government on national and local priorities for expanding universal and equitable access to ICTs, platforms and devices, and the underlying infrastructure to support them.

Investing in research

- Invest in evidence-based research and in-depth analysis of digital technologies, the impact of technologies on children, child protection and child rights considerations with regard to the digital environment, to integrate online protection systems into services used by children and young people.

Detailed information on the role of industry in Child Online Protection can be found in the industry specific guidelines.

International
Telecommunication
Union
Place des Nations
CH-1211 Geneva 20
Switzerland

Published in Switzerland
Geneva, 2020