

Executive summary  
**Guidelines for  
industry on Child  
Online Protection  
2020**





# Guidelines for industry on Child Online Protection

2020

# Introduction

---

As the Internet is fully integrated into children and young people's lives, it is impossible to consider the digital and physical worlds separately. In 2019, more than half of the world's population used the Internet. 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.

The Internet and 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. It can provide crucial access to health or educational services or information on topics that are important for young people but may be taboo in their societies.

Just as children and young people are often at the forefront of adopting and adapting to the new technologies and opportunities provided by the Internet, they are also being exposed to a range of content, contact and conduct threats and harms online.

With regard to protecting children's rights online, industries need to work together to strike a careful balance between children's right to protection and their right to access to information and freedom of expression. Companies should therefore prioritize measures to protect children and young people online that are targeted and are not unduly restrictive, either for the child or other users. Moreover, there is a growing consensus that promoting digital citizenship among children and young people, and developing products and platforms that facilitate children's positive use of information and telecommunication technologies (ICTs), should be a priority for the private sector.

These Guidelines for industry on Child Online Protection (COP) set a direction for industry stakeholders to build their own resources on COP, aiming to provide a useful, flexible and user-friendly framework for both enterprises' visions and their responsibility to protect their child users. They are also aimed at establishing the foundation for safer and more secure use of Internet-based services and associated technologies for today's children and future generations.

As a toolbox, these Guidelines also aim at enhancing business success by helping large and small operations and stakeholders to develop and maintain an attractive and sustainable business model, while understanding the legal and moral responsibilities towards children and society.



# Table of Contents

---

Introduction	ii
1 What is child online protection?	1
2 Key areas of protecting and promoting children's rights	1
3 General guidelines for all related industry	3
4 Feature-specific checklists	5





## 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. All relevant stakeholders have their role in helping children and young people benefit from the opportunities that the Internet can offer to them, while acquiring digital literacy and resilience for their digital well-being and protection.

While no universal definition exists for child online protection, it aims to take a holistic approach to building safe, age appropriate, inclusive and participatory digital spaces for children and young people, characterised by:

- response, support and self-help in the face of threat;
- prevention of harm;
- a dynamic balance between ensuring protection and providing opportunity for children to be digital citizens;
- upholding the rights and the responsibilities of both children and society.

Moreover, 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. New challenges will emerge with the development of technological innovations and will typically vary from region to region. These will be best dealt with by working together as a global community, as new solutions to these challenges need to be found.

## 2 Key areas of protecting and promoting children's rights

### **Integrating child rights considerations into all appropriate corporate policies and management processes**

Integrating child rights considerations requires that companies take adequate measures to identify, prevent, mitigate and, where appropriate, remediate potential and actual adverse impacts on children's rights. The United Nations Guiding Principles on Business and Human Rights call on all businesses and industries to put in place appropriate policies and processes to meet their responsibility to respect human rights.

### **Developing standard processes to handle child sexual abuse material (CSAM)**

In 2019, IWF actioned 132,676 webpages confirmed as containing child sexual abuse.<sup>1</sup> Any URL could contain hundreds, if not thousands, of images and videos. Of the images actioned by the IWF, 45 per cent showed children aged 10 or younger; and 1,609 webpages represented children aged 0–2 years, of which 71 per cent contained the most severe sexual abuse, such as rape and sexual torture. These disturbing facts underscore the importance of collaborative action among industry, governments, law enforcement and civil society to combat CSAM.

### **Creating a safer and age-appropriate online environment**

Children and young people can be thought of as receivers, participants and actors in their online environment. The risks that they face can be categorized into four areas:

- Inappropriate content

---

<sup>1</sup> IWF, "The why. The how. The who. And the results. Annual Report 2019".



- Inappropriate conduct
- Inappropriate contact
- Commercial risks

Online safety is a community challenge and an opportunity for industry, governments and civil society to work together to establish safety principles and practices. Industry can offer an array of technical approaches, tools and services for parents, and children and young people, and should first and foremost create products that are easy to use, safe and private by design and age-appropriate for their broad range of users. Children's safety and responsible use of technology has to be carefully considered and not be an afterthought. Acceptable-use policies are one way that companies can establish what type of behaviour by both adults and children is encouraged, what types of activities are not acceptable, and the consequences of any breaches to these policies. Clear reporting mechanisms should be made available to users who have concerns about content and behaviour. Services should be accompanied by user-friendly, easily understandable and accessible terms of content and security.

### **Educating children, carers and educators about children's safety and the responsible use of ICTs**

Parental control tools, awareness raising and education are also key components that will help empower and inform children and young people of all ages, as well as parents, caregivers and educators. Although companies have an important role in encouraging children and young people to use ICTs in a responsible and safe way, this responsibility is shared with parents, schools, and children and young people. It is also important to provide information directly to children and young people on safer ICT use and positive and responsible behaviour. Industry can work in collaboration with government and educators to strengthen parents' capacity to support their children in building their digital resilience and acting as responsible digital citizens. While children must be allowed to take some risks in the online environment, it is crucial that parents and companies can support them when things go wrong, as it can off-set the negative impact of an uncomfortable experience and turn it into a useful lesson for the future.

### **Promoting digital technology as a mode for increasing civic engagement**

Article 13 of the United Nations Convention on the Rights of the Child states that "the child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice." Companies can fulfil their duty to respect children and young people's civil and political rights by ensuring that technology, and the application of legislation and policies developed to protect children and young people from online harm do not have the unintended consequences of suppressing their right to participation and expression or preventing them from accessing information that is important for their well-being.

At the same time, businesses and industries can also support children and young people's rights by providing mechanisms and tools to facilitate youth participation. With the right tools and information, children and young people become empowered to access information about their rights and seek information about matters that affect them personally and about political and government accountability. Companies can also invest in the creation of online experiences appropriate for children and young people and families. They can support the development of technology and content that encourage and enable children and young people to learn, innovate and create solutions. Companies can, in addition, proactively support children and young people's rights by working to close the digital divide. Children and young people's participation requires digital literacy. Without this ability, citizens are not able to participate in many of the social functions that have become digitized. Companies can support multimedia initiatives to foster the digital skills that children and young people need to be confident, connected and actively involved citizens.



### 3 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.



**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.



**In collaboration with government, law enforcement, civil society and hotline organizations, industry 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 content 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:**

- 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:**

- 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.

## Guidelines for industry on Child Online Protection

- 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.

## 4 Feature-specific checklists

Complementing the previous general checklist for all related industry by offering recommendations for businesses that provide services with specific features on respecting and supporting children's rights online, the feature-specific Checklists offer recommendations for how businesses providing services with specific features can respect and support children's rights online further.

### **Feature A: Provide connectivity, data storage and hosting services**

Internet access is fundamental to the realization of children's rights, and connectivity can open up entire worlds for children. Providers of connectivity, data storage and hosting services have tremendous opportunities to build safety and privacy into their offers for children and young people, acting as both a conduit, providing access to and from the Internet, and a repository for data through their hosting, caching and storage services. As a result, they have had primary responsibility for protecting children online.

This service feature addresses, among others, mobile operators, Internet service providers, data storage systems and hosting services.

### **Feature B: Offer curated digital content**

The Internet provides all types of content and activities, many of which are intended for children and young people. Services offering editorially curated content have tremendous opportunities to build safety and privacy into their offers for children and young people.

This service feature addresses both businesses that are creating their own content, and those that are enabling access to digital content. It refers to, inter alia, news and multimedia streaming services, national and public service broadcasting and the gaming industry.

### **Feature C: Host user-generated content and connect users.**

There was a time when the online world was dominated by adults, but it is now clear that children and young people are major participants, on multiple platforms, in creating and sharing in the explosion of user-generated content. This service feature addresses among others but is not limited to social media services, apps and websites related to creative realization.

Services that connect users with each other can be divided in three categories:

- Primarily messaging apps.
- Primarily social networking services that seek and host user-generated content and allow users to share content and connect within and outside of their networks.
- Primarily live streaming apps.

### **Feature D: Artificial intelligence-driven systems**

With the increased attention given to deep learning technologies, the terms "artificial intelligence", "machine learning", and "deep learning" have been used somewhat interchangeably by the general public to reflect the concept of replicating "intelligent" behaviour in machines. In this section, we focus on the ways that machine learning and deep learning processes impact children's lives and ultimately, their human rights.



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

Published in Switzerland  
Geneva, 2020