ITU Publications

International Telecommunication Union
Development sector

Guidelines for industry on Child Online Protection

2020

Guidelines for industry on Child Online Protection

Acknowledgements

These guidelines have been developed by the International Telecommunication Union (ITU) and a working group of contributing authors from leading institutions active in the sector of information and communication technologies (ICT) as well as child protection issues and included the EBU, the Global Partnership to End Violence Against Children, GSMA, the International Disability Alliance, the Internet Watch Foundation (IWF), Privately SA and UNICEF. The working group was chaired by Anjan Bose (UNICEF) and coordinated by Fanny Rotino (ITU).

These ITU guidelines would not have been possible without the time, enthusiasm and dedication of the contributing authors. Invaluable contributions were also received from the e-Worldwide Group (e-WWG), Facebook, Tencent Games, Twitter, the Walt Disney Company, as well as other industry stakeholders, that share a common objective of making the Internet a better and safer place for children and young people. ITU is grateful to the following partners, who contributed their valuable time and insights (listed in alphabetical order of the organizations):

- Giacomo Mazzone (EBU)
- Salma Abbasi (e-WWG)
- David Miles and Caroline Hurst (Facebook)
- Amy Crocker and Serena Tommasino (Global Partnership to End Violence Against Children)
- Jenny Jones (GSMA)
- Lucy Richardson (International Disability Alliance)
- Fanny Rotino (ITU)
- Tess Leyland (IWF)
- Deepak Tewari (Privately SA)
- Adam Liu (Tencent Games)
- Katy Minshall (Twitter)
- Anjan Bose, Daniel Kardefelt Winther, Emma Day, Josianne Galea Baron, Sarah Jacobstein and Steven Edwin Vosloo (UNICEF)
- Amy E. Cunningham (The Walt Disney Company)

ISBN

978-92-61-30081-4 (Paper version)

978-92-61-30411-9 (Electronic version)

978-92-61-30071-5 (EPUB version)

978-92-61-30421-8 (Mobi version)

Please consider the environment before printing this report.

Foreword

The explosion in digital technologies has created unprecedented opportunities for children and young people to communicate, connect, share, learn, access information and express their opinions on matters that affect their lives and their communities.

But wider and more easily available access to online services also poses significant challenges to children's safety – both online and offline. From issues of privacy, peer-to-peer-violence, and violent and/or age-inappropriate content, to Internet scammers and crimes against children such as online grooming, and sexual abuse and exploitation, today's children face many serious risks. Threats are multiplying and perpetrators increasingly operate simultaneously across borders, making them hard to track and even harder to hold to account.

In addition, the COVID-19 global pandemic saw a surge in the number of children joining the online world for the first time, to support their studies and maintain social interaction. The constraints imposed by the virus not only meant that many younger children began interacting online much earlier than their parents might have planned but also that the need to juggle work commitments left many parents unable to supervise their children, leaving young people at risk of accessing inappropriate content or being targeted by criminals in the production of child sexual abuse material (CSAM).

Criminals are profiting from technological advances, such as inter-connecting apps and games, fast file sharing, live streaming, cryptocurrencies, the Dark Web, and strong encryption software. However, they are also profiting from often uncoordinated and hesitant action on the part of the tech sector to effectively combat the problem.

Emerging technologies can be a part of the solution, for example Interpol's artificial intelligence-based child sexual abuse database that uses image and video comparison software to quickly make connections between victims, abusers and places. But technology alone will not solve the problem.

To reduce the risks of the digital revolution while enabling more and more young people to reap its benefits, a collaborative and coordinated multi-stakeholder response has never been more essential. Governments, civil society, local communities, international organizations and industry stakeholders must all come together in common purpose.

Recognizing this, in 2018, ITU Member States requested a comprehensive updating of our guidelines on child online protection. These new ITU guidelines have been rethought, rewritten and redesigned to reflect the very significant shifts in the digital landscape in which this generation's children find themselves. In addition to reflecting new developments in digital technologies and platforms, this new edition addresses an important lacuna: the situation faced by children with disabilities, for whom the online world offers a particularly crucial lifeline to full – and fulfilling – social participation.

The technology industry has a critical and proactive role to play in establishing the foundations for safer and more secure use of Internet-based services and other technologies, for today's children and future generations.

Business must increasingly put children's interests at the heart of its work, paying special attention to protecting the privacy of young users' personal data, preserving their right to freedom of expression, combating the growing scourge of CSAM and ensuring there are systems in place to effectively address violations of children's rights when they occur.

Where domestic laws have not yet caught up with international law, every business has an opportunity – and a responsibility – to bring its own operational frameworks into line with the very highest standards and best practices.

For industry, we hope these guidelines will serve as a solid foundation on which to develop business policies and innovative solutions. In the true spirit of the ITU role as a global convener, I am proud that these guidelines are the product of a global collaborative effort and have been co-authored by experts drawn from a broad international community.

I am also delighted to introduce our new COP mascot, Sango: a friendly, feisty and fearless character designed entirely by a group of children as part of the ITU new international youth outreach programme.

In an age where more and more young people are coming online, the ITU child protection guidelines are more important than ever. Industry, governments, parents and educators, as well as children themselves, all have a vital role to play. I am grateful, as always, for your support and I look forward to continuing our close collaboration on this critical issue.

Doreen Bogdan-Martin
Director
Telecommunication Development Bureau, ITU

Table of Contents

Table

1. Overview

The purpose of this document is to provide a direction for ICT industry stakeholders to build their own child online protection (COP) resources. The aim of these guidelines for industry on child online protection is to provide a useful, flexible and user-friendly framework for both enterprise visions and their responsibility to protect 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.

In response to substantial advances in technology and convergence, ITU, UNICEF and child online protection partners have developed and updated the guidelines for the broad range of companies that develop, provide or use telecommunications or related activities in the delivery of their products and services.

The new guidelines for industry on child online protection are the result of consultations with members of the COP Initiative, as well as wider consultations with members of civil society, business, academia, governments, media, international organizations and young people.

The purpose of this document is to:

- establish a common reference point and guidance for the ICT and online industries and relevant stakeholders;
- provide guidance to companies on identifying, preventing and mitigating any adverse impacts of their products and services on children's rights;
- provide guidance to companies on identifying ways in which they can promote children's rights and responsible digital citizenship among children;
- suggest common principles to form the basis of national or regional commitments across all related industries, while recognizing that different types of businesses will use diverse implementation models.

Scope

Child online protection is a complex challenge that encompasses multiple different governance, policy, operational, technical and legal aspects. These guidelines attempt to address, organize and prioritize many of these areas, based on existing and well recognized models, frameworks and other references.

The guidelines focus on protecting children in all areas and against all risks of the digital world and, as such, highlight good practice of industry stakeholders that can be considered in the process of drafting, developing and managing company COP policies. They provide guidance to industry actors not only on how to manage and contain illegal online activity against which they have a duty to act (such as online CSAM) through their services, but also focus on other issues which may not be defined as crimes across all jurisdictions. These include peer-to-peer violence, cyberbullying and online harassment, as well as issues related to privacy or general well-being, fraud or other threats, which may only be harmful to children in certain contexts.

To this end, these guidelines include recommendations on good practice in meeting the risks children face in the digital world and how to act in order to establish a secure environment for children online. These guidelines provide advice on how industry can work to help ensure children's safety when using ICTs, the Internet or any of the associated technologies or devices that can connect to it, including mobile phones, game consoles, connected toys, watches, the Internet of things and AI-driven systems. They therefore provide an overview of the key issues and challenges regarding child online protection and propose actions for businesses and stakeholders for the development of local and internal COP policies. These guidelines do not cover aspects such as the actual development process or text that COP policies for industry could include.

Structure

Section 1 – Overview: This section highlights the purpose, scope and target audience of these guidelines.

Section 2 – Introduction to child online protection: This section sets out an overview of the issue of child online protection, outlining some background information, including the special situation of children with disabilities. Moreover, it provides examples of existing international and national models to keep children safe online as possible areas of intervention for industry stakeholders.

Section 3 – Key areas of protecting and promoting children's rights: This section outlines five key areas where companies can take action to ensure children's safe and positive use of ICTs.

Section 4 – General guidelines: This section provides recommendations for all industry stakeholders on protecting children's safety when using ICTs and on promoting positive ICT use, including responsible digital citizenship among children.

Section 5 – Feature-related checklists: This section highlights specific recommendations for stakeholders on concrete actions to respect and support children's rights, with the following features:

- Feature A: Provide connectivity, data storage and hosting services
- Feature B: Offer curated digital content
- Feature C: Host user-generated content and connect users
- Feature D: AI-driven systems

Target audience

Building on the United Nations Guiding Principles on Business and Human Rights,[1] the Children's Rights and Business Principles call on businesses to meet their responsibility to respect children's rights by avoiding any adverse impacts linked to their operations, products or services. These Principles also articulate the difference between respect (the minimum required of business to avoid causing harm to children) and support (for example, by taking voluntary actions that seek to advance the realization of children's rights). Businesses need to ensure children's right both to online protection as well as to access to information and freedom of expression, while promoting children's positive use of ICTs.

[1] United Nations Guiding Principles on Business and Human Rights.

Traditional distinctions between different parts of the telecommunications and mobile phone industries, and between Internet companies and broadcasters, are fast breaking down and becoming blurred. Convergence is drawing these previously disparate digital streams into a single current that is reaching billions of people in all parts of the world. Cooperation and partnership are the keys to establishing the foundations for safer and more secure use of the Internet and associated technologies. Governments, the private sector, policy-makers, educators, civil society, parents and caregivers all have a vital role in achieving this goal. Industry can act in five key areas, as described in section 3.

2. What is child online protection?

Over the last 10 years, the use and role of the Internet in people's lives has changed considerably. With the prevalence of smartphones and tablets, the accessibility of Wi-Fi and 4G technology, and developments in social media platforms and apps, more and more people are accessing the Internet for ever-increasing reasons.

In 2019, over half of the world's population used the Internet. The largest proportion of Internet users are people under 44 years, with Internet use equally high among 16–24 year-olds and 35–44 year-olds. At the global level, one in three Internet users is a child (0–18 years) and UNICEF estimates that 71 per cent of young people are already online.[2] The proliferation of Internet access points, mobile technology and the growing array of Internet-enabled devices, combined with the immense resources to be found in cyberspace, provide unprecedented opportunities to learn, share and communicate.

The benefits of ICT usage include broader access to information on social services, educational resources and health advice. As children and young people and families use the Internet and mobile phones to seek information and assistance, and to report incidents of abuse, these technologies can help to protect children and young people from violence and exploitation. Child protection service providers also use ICTs to gather and transmit data, thereby facilitating birth registration, case management, family tracing, data collection and mapping of violence, among others.

Moreover, the Internet has increased access to information in all corners of the globe, enabling children and young people to research almost any subject of interest, access worldwide media, pursue vocational prospects and harness ideas for the future. ICT usage empowers children and young people to assert their rights and express their opinions, and also allows them to connect and communicate with their families and friends. ICTs also serve as a paramount mode of cultural exchange and a source of entertainment.

Despite the profound benefits of the Internet, children and young people can also encounter a number of risks when using ICTs. They can be exposed to age-inappropriate content or inappropriate contact, including from potential perpetrators of sexual abuse. They can suffer reputational damage from publishing sensitive personal information either online or through "sexting", often failing to comprehend the implications of their actions on themselves and

[2] OECD, "New Technologies and 21st Century Children: Recent Trends and Outcomes", Education Working Paper No. 179.

others and their long-term "digital footprints". They also face risks related to online privacy stemming from data collection, and collection and use of location information.

The Convention on the Rights of the Child, which is the most widely ratified international human rights treaty,[3] sets out the civil, political, economic, social, and cultural rights of children. It establishes that all children and young people have the right to education; leisure, play and culture; appropriate information; freedom of thought and expression; and privacy, and to express their views on matters that affect them in accordance with their evolving capacities. The Convention also protects children and young people from all forms of violence, exploitation, abuse and discrimination of any kind, and sets out that the child's best interest should be the primary consideration in any matters affecting them. Parents, carers, educators and community members, including community leaders and civil society actors, have the responsibility to nurture and support children and young people in their passage to adulthood. Governments have an important role in ensuring that all such stakeholders fulfil this role.

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 ICTs, should be a priority for the private sector.

While online technologies present many opportunities for children and young people to communicate, learn new skills, be creative and contribute to improving society for all, they can also pose new risks to the safety of children and young people. They can expose children and young people to potential risks and harms related to issues of privacy, illegal content, harassment, cyberbullying, misuse of personal data or grooming for sexual purposes and even child sexual abuse and exploitation. They may also be exposed to reputational damage including "revenge porn" linked to publishing sensitive personal information either online or through "sexting", a way for users to send sexually explicit messages, photographs or images between mobile phones. They also face risks related to online privacy when using the Internet. Children, by nature of their age and developing maturity, are often unable to fully comprehend the risks associated with the online world and the possible negative repercussions of their inappropriate behaviour on others and themselves.

Despite the advantages, there are also downsides to the use of emerging and more-advanced technologies. Developments in AI and machine learning, virtual and augmented reality, big data, robotics and the Internet of Things are set to transform children and young people's media practices even further. While these technologies are predominantly being developed to expand the scope of service delivery and enhance convenience (through, for example, voice assistance, accessibility and new forms of digital immersion), some such technologies could have unintentional impacts and even be misused by child sex offenders to serve their needs. Creating a safe and secure online environment for children and youth requires the effective participation of governments, the private sector and all stakeholders. Focusing on the digital skills and literacy of parents and educators must also be one of the first targets, in the achievement of which industry can play a vital and sustainable role.

[3] United Nations Convention on the Rights of the Child. All but three countries (Somalia, South Sudan and the United States) have ratified the Convention on the Rights of the Child.

Some children may have a good understanding of online risks and how to respond to them. However, this cannot be said of all children everywhere, particularly among vulnerable groups. Under target 16.2 of the United Nations Sustainable Development Goals, which aims to end abuse, exploitation, trafficking and all forms of violence and torture against children, protection of children online is vital.

Since 2009, the COP Initiative, an international multi-stakeholder effort established by ITU, has aimed to raise awareness of risks to children online and responses to those risks. The Initiative brings together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere. As part of the Initiative, in 2009 ITU published a set of COP guidelines for four groups: children; parents, guardians and educators; industry; and policy-makers. Child online protection is understood in these guidelines as an all-inclusive approach to respond to all potential threats and harms that children and young people may encounter either online or facilitated by online technologies. In this document, child online protection also includes harm to children that occurs offline but is linked to evidence of online violence and abuse. In addition to the consideration of children's online behaviour and activities, child online protection also refers to the misuse of technology by persons other than the children themselves to exploit children.

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

Protecting children and young people is the shared responsibility of all stakeholders. For that to happen, policy-makers, industry, parents, carers, educators and other stakeholders, must ensure that children and young people can fulfil their potential – online and offline.

While no there is no universal definition, child online protection takes a holistic approach to building safe, age appropriate, inclusive and participatory digital spaces for children and young people, characterized by:

- response, support and self-help in the face of threats;
- prevention of harms;
- a dynamic balance between ensuring protection and providing opportunity for children to become 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 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.

2.1 Background information

As the Internet is fully integrated into children and young people's lives, it is impossible to consider the digital and physical worlds separately.

Such connectivity has been tremendously empowering. The online world allows children and young people to overcome disadvantages and disabilities, and has provided new arenas for

entertainment, education, participation and relationship building. Current digital platforms are used for a variety of activities and are often multi-media experiences.

Having access to and learning to use and navigate this technology is seen as critical to young people's development and ICTs are first used at an early age. It is thus crucial that all actors are aware that children and young people often start using platforms and services before they reach the defined minimum age with which the tech industry is required to comply and, therefore, education should be integrated into all online services used by children alongside protection measures.

2.1.1 Children in the digital world

Internet access

In 2019, more than half of the world's population used the Internet (53.6 per cent), with an estimated 4.1 billion users. At the global level, one-in-three Internet users is a child under 18 years of age[1]. According to UNICEF, worldwide, 71 per cent of young people are already online[2]. Despite the minimum age requirements, Ofcom (United Kingdom communications regulator) estimates that nearly 50 per cent of children between 10 and 12 years already have a social media account.[3] Children and young people are now a substantial, permanent and persistent presence on the Internet. The Internet serves other social, economic and political purposes and has become a family or consumer product or service, integral to the way families, children and young people live their lives.

In 2017, at the regional level, children and young people's access to the Internet was strongly linked to the level of national income. Low-income countries tend to have lower levels of child Internet users than high-income countries. Children and young people in most countries spend more time online at weekends than weekdays, with adolescents aged 15–17 years spending the longest periods online, at between 2.5 and 5.3 hours, depending on the country.

---

1 Livingstone, S., Carr, J., and Byrne, J. (2015) One in three: The task for global internet governance in addressing children's rights. Global Commission on Internet Governance: Paper Series. London: CIGI and Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

2 Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)," *Broadband Commission for Sustainable Development,* October 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

3 BBC, "Under-age social media use 'on the rise', says Ofcom".

Internet use

Among children and young people, the most popular device for accessing the Internet is the mobile phone, followed by desktop computers and laptops. Children and young people spend on average two hours a day online during the week and four hours each day of the weekend. While some feel permanently connected, many others still do not have access to the Internet at home. In practice, most children and young people who use the Internet gain access through more than one device, with those who connect at least weekly sometimes using up to three different devices. Older children and those in richer countries generally use more devices, and boys use slightly more devices than girls in every country surveyed.

The most popular activity among both girls and boys is watching video clips. More than three quarters of Internet-using children and young people report watching videos online at least weekly, either alone or with other members of their family. Many children and young people can be considered "active socializers", using several social media platforms such as Facebook, Twitter, Tiktok or Instagram. Children and young people also engage in politics online and make their voices heard through blogging.

The overall level of participation in online gaming varies by country roughly in line with ease of access to the Internet for children and young people. However, the availability and affordability of online games are rapidly changing and the age of children and young people first accessing online gaming is decreasing.

On a weekly basis, 10-30 per cent of Internet-using children and young people – consulted in a selected set of countries - engage in creative online activities.[1] For educative purposes, many children and young people of all ages use the Internet for homework, or even to catch up after missing classes or seek health information online, on a weekly basis. Older children seem to have a greater appetite for information than younger children.

[1] Livingstone, S., Kardefelt Winther, D., and Hussein, M. (2019). *Global Kids Online Comparative Report, Innocenti Research Report*. UNICEF Office of Research - Innocenti, Florence, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html.

Online child sexual exploitation and abuse

Online child sexual exploitation and abuse (CSEA) is rising at a startling rate. A decade ago there were fewer than one million files of child abuse material reported. In 2019, that number had climbed to 70 million, a nearly 50 per cent increase over 2018 figures. In addition, for the first time videos of abuse have outnumbered photos in reports to the authorities, showing the need for new tools to address this trend. Victims of online CSEA fall into all age groups but are increasingly younger. In 2018, the INHOPE network of hotlines noted a shift in victim profiles from pubescent to prepubescent. In addition, research by ECPAT International and INTERPOL in 2018 found that younger children were more likely to suffer severe abuse, including torture, violent rape or sadism. This includes infants who are only days, weeks or months old. While girls are more affected, abuse of boys may be more severe. The same report shows that 80 per cent of victims referred to in reports were girls and 17 per cent were boys. Children of both genders were mentioned in 3 per cent of assessed reports.[1]

Data Snapshot[2]

- One in three Internet users worldwide is a child.
- Every half second, a child goes online for the first time.
- 800 million children use social media.
- At any one time, 750,000 individuals online are estimated to be looking to connect with children for sexual purposes.
- There are more than 46 million unique images or videos of CSAM in the EUROPOL repository.
- Over 89 per cent of victims are aged between 3 and 13 years old.

For more information about the scale and response to online CSEA see the WePROTECT Global Alliance.

1 ECPAT and Interpol, "Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: summary report", 2018.
2 End Violence Against Children, "Safe Online".

2.1.2 The impact of different platforms on children's digital experiences

The Internet and digital technology present both opportunities and risks to children and young people. Some of these are outlined below.

When children use **social media**, they benefit from many opportunities to explore, learn, communicate and develop key skills. Social networks are seen by children as platforms that allow them to explore their personal identity in a safe environment. Having the relevant skills and knowing how to tackle issues related to privacy and reputation is important for young people.

"I know everything you post on the Internet stays there forever and it can affect your life in the future", 14-year-old boy, Chile.

However, with surveys showing that most children are using social media before the minimum age of 13 and age verification services being generally weak or lacking, the risks facing children can be serious. Furthermore, while children want to learn digital skills, become digital citizens and control privacy settings, they tend to consider privacy in relation to their friends and acquaintances – "What can my friends see?"- and less so in relation to strangers and third parties. This, combined with children's natural curiosity and generally lower threshold for risk, can make them vulnerable to grooming, exploitation, bullying or other types of harmful content or contact.

The widespread popularity of image and video sharing via mobile apps, and particularly the use of live streaming platforms by children, presents further privacy concerns and risks. Some children are producing sexual images of themselves, friends and siblings and sharing them online. In 2019, almost a third (29 per cent) of all webpages captioned by the IWF contained self-generated imagery. Of those, 76 per cent showed girls aged 11–13, with most in their bedrooms or another room in a home setting. For some, particularly older children, this can be seen as the natural exploration of sexuality and sexual identity, while for others, particularly younger children, there is often coercion by an adult or other child. Whatever the case, the resulting content is in many countries illegal and may expose children to the risk of prosecution or be used to further exploit, groom or extort the child.

Similarly, **online gaming** enables children to fulfil their fundamental right to play, as well as build networks, spend time with friends and meet new ones, and develop important skills. While this can be overwhelmingly positive, in some cases, left unmonitored and unsupported by a responsible adult, gaming platforms can also pose risks to children. This includes playing excessively, financial risks linked to excessive in-game purchases, collection and monetization of children's personal data by industry actors, cyberbullying, hate speech, violence and exposure to inappropriate conduct or content, grooming, using real, computer-generated or even virtual reality images, and videos depicting and normalizing CSEA. These risks are not unique to the gaming environment but apply to other digital environments where children spend time.

Furthermore, developments in technology have led to the emergence of the "**Internet of Things**", where an increasing number and range of Internet-connected devices are able to communicate and network over the Internet. This includes toys, baby monitors and devices powered by AI that may present risks in terms of privacy and unwanted contact.

Good practice: Research

In the context of online or cyberbullying, Microsoft has conducted research into digital safety and cyberbullying. In 2012, it polled children aged 8–17 years in 25 countries about negative behaviour online. The results showed that, on average, 54 per cent of participants indicated that they were worried they would be bullied online; 37 per cent indicated that they had been cyberbullied; and 24 per cent revealed that they had bullied someone. The same survey demonstrated that fewer than three in 10 parents had discussed online bullying with their children. Since 2016, Microsoft has been conducting **regular research** into online risks providing yearly Digital Civility Index reports.

FACES is a multimedia programme produced by NHK Japan and by a consortium of various public service broadcasters with stories of victims of online and offline bullying across the world. A series of portraits of adolescents in which the protagonists explain to camera how they reacted to attacks over the Internet. The series, produced also in two-minute clips, have been adopted by Facebook, UNESCO, and the Council of Europe, and is available in many languages.

In 2019, UNICEF published a discussion paper on Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry to address the opportunities and challenges for children in one of the fastest growing entertainment industries. The paper explores the following topics:

- Children's right to play and freedom of expression (gaming time and health outcomes);
- Non-discrimination, participation and protection from abuse (social interaction and inclusion, toxic environments, age limits and verification, protection from grooming and sexual abuse);
- The right to privacy and freedom from economic exploitation (data-for-access business models, free-to-play games and monetization, lack of transparency in commercial content).

Good practice: Technology

The Google Virtual Reality Action Lab examines how virtual reality can help encourage youth to become upstanders against offline and online bullying.[1]

In September 2019, the BBC launched a mobile application called **Own IT**, a well-being app aimed at children aged 8–13 receiving their first smartphone. The app is part of the BBC's commitment to supporting young people in today's changing media environment and follows the successful launch of the Own IT website in 2018. The app combines state-of-the-art machine-learning technology to track children's activity on their smartphone with the option for children to self-report their emotional state. It uses this information to deliver tailored content and interventions to help children stay happy and healthy online, offering friendly and supportive nudges when their behaviour strays outside the norm. Users can access the app when they are looking for help but it is also on hand to give instant, on-screen advice and support when they need it, via a specially developed keyboard. Features include:

- Reminding users to think twice before sharing personal details like mobile numbers on social media.
- Helping them understand how messages could be perceived by others, before they hit send.
- Tracking their mood over time and offering guidance on how to improve the situation if needed.
- Providing information on topics like using phones late at night and the impact on users' well-being.

The app features specially commissioned content from across the BBC. It provides useful material and resources to help young people get the most out of their time online and build healthy online behaviour and habits. It helps young people and parents have more constructive conversations about their experiences online but will not provide reports or feedback to parents and no data will leave users' devices. The app does not collect any personal data or content generated by the user, as the entire machine learning runs within the app and within the device of the user. The machines are trained separately on training data in order to assure that there are no privacy violations.

[1] For more information see, Alexa Hasse et al., "Youth and Cyberbullying: Another Look", Berkman Klein Center for Internet & Society, 2019.

2.1.3 The special situation of children with disabilities [4]

Children and young people with disabilities face risks online similarly to those without disabilities but, additionally, they may face specific risks related to their disabilities. Children and young people with disabilities often face exclusion, stigmatization and barriers (physical, economic, societal and attitudinal) to participating in their communities. These experiences can have a negative impact on a child with a disability and lead him or her to seek out social

[4] See Council of Europe, "Two clicks forward and one click back: report on children with disabilities in the digital environment", 2019.

interactions and friendships in online spaces. While such interactions can be positive by assisting in building self-esteem and creating support networks, they can also place such children at higher risk of incidents of grooming, online solicitation and/or sexual harassment. Research shows that children and young people experiencing difficulties offline and those affected by psychosocial difficulties are at heightened risk of such incidents.[5]

Overall, children who are victimized offline are likely to be victimized online. This places children with disabilities at higher risk online, yet they have a greater need to be online. Research shows that children with disabilities are more likely to experience abuse of any kind,[6] specifically sexual victimization.[7] Victimization can include bullying, harassment, exclusion and discrimination based on a child's actual or perceived disability or on aspects related to their disability, such as the way that they behave or speak, or equipment or services they use.

Perpetrators of grooming, online solicitation and/or sexual harassment towards children and young people with disabilities can include not only preferential offenders who target children and young people, but also those who target children and young people with disabilities. Such offenders may include "devotees" – non-disabled persons sexually attracted to persons with disabilities (most commonly amputees and persons using mobility aids), some of whom even pretend to be disabled themselves.[8] Actions by such people may include downloading photos and videos of children and young people with disabilities (that are innocuous in nature) and/or sharing them through dedicated forums or social media accounts. Reporting tools on forums and social media often do not have an appropriate pathway to deal with such actions.

There are concerns that "sharenting" (parents sharing information and photos of their children and young people online) can violate a child's privacy, lead to bullying, and embarrassment, or have negative consequences later in life.[9] Some parents of children with disabilities may share information or media of their child in pursuit of support or advice, as a result, placing their child at risk of privacy violations both now and in the future. Such parents also risk being targeted by uninformed or unscrupulous people offering treatments, therapies or "cures" for a child's disability. Equally, some parents of children and young people with disabilities may be overprotective because of their lack of knowledge on how to best guide their child's use of the Internet or protect them from bullying or harassment.[10]

Some children and young people with disabilities may face difficulties in using, or even exclusion from, online environments due to inaccessible designs (e.g. apps that don't allow text size to be increased), denial of requested accommodations (e.g. screen reader software or adaptive computer controls), or the need for appropriate support (e.g. coaching in how to use equipment, one-on-one support to navigating social interactions).[11]

---

5 Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content", Berkman Center for Internet & Society, 2008.

6 UNICEF, "State of the World's Children Report: Children with Disabilities," 2013.

7 Katrin Mueller-Johnson et al., "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors", Journal of Interpersonal Violence, 2014.

8 Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder", Sexuality and Disability, 1997.

9 UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy", Innocenti Discussion Paper 2017-03 .

10 UNICEF, "Is there a ladder of children's online participation?", Innocenti Research Brief, 2019.

11 For guidelines on these rights, see the United Nations Convention on the Rights of Persons with Disabilities and Optional Protocol, especially Article 9 on accessibility and Article 21 on freedom of expression and opinion, and access to information.

2.2 Existing national and transnational models for Child Online Protection

At the global level, several models are being adopted to keep children and young people safe online. Industry stakeholders should consider these as guidance for international initiatives and as a framework to ensure they spare no efforts to protect children and young people online. The Internet industry is a diverse and intricate arena, compiled of companies of different sizes and functions. It is essential that child protection is addressed not only by platforms and services based around content but also by those supporting the infrastructure of the Internet.

It must be noted that the capacity of an industry to introduce a comprehensive child protection policy is limited to its available resources. These guidelines, therefore, recommend that industries work together to deploy services to protect users. By sharing resources and engineering expertise, industries would be able to more effectively create "safe spaces" to prevent abuse.

Industry cooperation

The Technology Coalition is an example of successful cooperation between industry stakeholders to fight CSEA.

Transnational models

Industries should include relevant international guidelines in their structural programme as well as abide by any relevant national or transnational legislation that applies in the countries in which they operate. Industries should not only consider the actions they must take at the legal level but also what activities they can perform and, where possible, seek to implement initiatives globally. Some of the models that provide principles for such initiatives include:

- Five Country Ministerial Voluntary principles to counter online CSEA (2020);
- Broadband Commission for Sustainable Development, Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019);
- WePROTECT Global Alliance, A Global Strategic Response to Online Child Sexual Exploitation and Abuse (2019);
- Global Partnership to End Violence against Children, Safe to Learn: Call to Action;
- Child Dignity in the Digital World, Child Dignity Alliance: Technology Working Group Report (2018);
- Directive (EU) 2018/1808 of the European Parliament and of the Council: Audio Visual Media Services Directive;
- European Commission General Data Protection Regulation (2018);
- OECD Recommendation on Protection of Children Online (2012).

National models

There are a number of national and international models that set out the clear roles and responsibilities of the technology industry in addressing child online protection. Some of these are not specific to children per se but can apply to them as Internet users. They provide overarching guidelines to the industry regarding regulatory policies, standards and collaboration with other sectors. For the purpose of this document, the key principles of such models, as they apply to the ICT industry, are highlighted.

The Age Appropriate Design Code, the United Kingdom

In early 2019, the Information Commissioner's Office published proposals for its age-appropriate design code on the protection of childrens's data. The proposed code is based on the best interests of the child, as laid out in the United Nations Convention on the Rights of the Child, and sets out several expectations for industry. The code consists of fifteen standards including, location services to be off by default for children, for industry to collect and retain only the minimum amount of personal data of children, for products to be private by design and for explanations to be age-appropriate and accessible.

The Harmful Digital Communications Act, New Zealand

The 2015 Act made cyber abuse a specific crime and focuses on a broad range of harms, from cyberbullying to revenge pornography. It aims to deter, prevent and lessen digital communication that is harmful, making it illegal to post a digital communication with the intention of causing serious emotional distress to someone else, and sets out a series of 10 communication principles. It empowers users to complain to an independent organization if these principles are broken or apply for court orders against the author or host of the communication if the issue is not resolved.

The eSafety Commissioner, Australia

Established in 2015, the Australia eSafety Commissioner is the world's first government agency dedicated to tackling online abuse and keeping its citizens safer online. As the national independent regulator for online safety, eSafety has a powerful combination of functions. These range from prevention through awareness-raising, education, research and best practice guidance, to early intervention and harm remediation through multiple statutory regulatory schemes that give eSafety the power to rapidly remove cyberbullying, image-based abuse and illegal online content. This broad remit enables eSafety to address online safety in a multifaceted, holistic and proactive way.

In 2018, eSafety developed Safety by Design (SbD), an initiative that places the safety and rights of users at the centre of the design, development and deployment of online products and services. A set of safety by design principles sit at the heart of the initiative, which set out realistic, actionable and achievable measures for industry to undertake to better protect and safeguard citizens online. The three overarching principles are:

1) **Service provider responsibilities**: the burden of safety should never fall solely upon the end-user. Preventative steps can be taken to ensure that known and anticipated harms have been evaluated in the design and provision of an online service, along with steps to make services less likely to facilitate, inflame or encourage illegal and inappropriate behaviours.
2) **User empowerment and autonomy**: the dignity of users and their best interests are of central importance. Human agency and autonomy should be supported, amplified and strengthened in service design allowing users greater control, governance and regulation of their own experiences.
3) **Transparency and accountability**: these are hallmarks of a robust approach to safety, that provide assurances that services are operating according to their published safety objectives, as well as educating and empowering the public about steps that can be taken to address safety concerns.

The WePROTECT Global Alliance

At the heart of the WePROTECT Global Alliance strategy are supporting countries to develop coordinated multi-stakeholder responses to tackle online child sexual exploitation, guided by its Model National Response, which acts as a blueprint for national action. It provides a framework for countries to draw upon to tackle online child sexual exploitation. Within the WePROTECT Model National Response, there is a clear set of commitments from ICT companies relating to:

- notice and takedown procedures;
- report online child sexual exploitation and abuse (CSEA);
- develop technology solutions; and
- invest in effective COP preventive programmes and response services.

The Global Partnership and Fund to End Violence against Children

The Global Partnership and Fund to End Violence against Children were launched by the United Nations Secretary-General in 2016 with one goal: to catalyze and support action to end all forms of violence against children by 2030 through a unique collaboration of over 400 partners from all sectors.

The focus of the work is on rescue and support of victims, technology solutions to detect and prevent offending, support of law enforcement, legislative and policy reforms, and generation of data and evidence on the scale and nature of online CSEA as well as understanding children's perspectives.[12]

3. Key areas of protecting and promoting children's rights

This section outlines **five key areas** where companies can take actions to protect children and young people's safety when using ICTs and promote their positive use of ICTs.

3.1 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.

[12] For more information see End Violence Against Children, "Grantees of the End Violence Fund".

Industries should pay special attention to children and young people as a vulnerable group with regard to their data protection and freedom of expression. The United Nations General Assembly Resolution 68/167 on the right to privacy in the digital age reaffirms the right to privacy and freedom of expression without being subjected to unlawful interference. Additionally, the United Nations Human Rights Council Resolution 32/13 on the promotion, protection and enjoyment of human rights on the Internet, recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development and affirms that the same rights people have offline must also be protected online. In States where there is a lack of adequate legal frameworks for the protection of children and young people's rights to privacy and freedom of expression, the companies should follow enhanced due diligence to ensure policies and practices are in line with international law. As youth civic engagement continues to increase through online communications, companies have a greater responsibility to respect children and young people's rights, even where domestic laws have not yet caught up with international standards.

Companies should have in place an operational-level grievance mechanism to provide a format for affected individuals to raise concerns of potential violations. Operational level mechanisms should be accessible to children, their families and those who represent their interests. Principle 31 of the Guiding Principles on Business and Human Rights clarifies that such mechanisms should be legitimate, accessible, predictable, equitable, transparent, rights-compatible, a source of continuous learning, and based on engagement and dialogue. Together with internal processes to address negative impacts, grievance mechanisms should ensure that companies have frameworks in place to ensure children and young people have suitable recourse when their rights have been threatened.

When companies take a compliance-based approach towards ICT safety that focuses on meeting national legislation, following international guidance when national legislation is not present, and avoiding adverse impacts on children and young people's rights, companies proactively promote children and young people's development and well-being through voluntary actions that advance children and young people's rights to access information, freedom of expression, participation, education and culture.

Good practice: Policy and age-appropriate design

The app developer Toca Boca produces digital toys from the child perspective. The company privacy policy is designed to share what information the company collects and how it is used. Toca Boca, Inc is a member of the PRIVO Kids Privacy Assured COPPA Safe Harbor Certification Program.

LEGO® Life is an example of safe social media platform for children under the age of 13 years to share their LEGO creations, get inspired and interact safely. Children here are not asked for any personal information to create an account, which is possible only with the email address of a parent or carer. The App creates an opportunity for children and families to discuss online safety and privacy in a positive environment.

Examples of age-appropriate design include specific offers of some of the major Public Service Broadcasters for certain age groups: for example, the German ARD (Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland – Das Erste) and ZDF (Zweites Deutsches Fernsehen) target their audience starting from 14 years old, offering customized content through the online channel funk.net. The BBC (British Broadcasting Corporation) launched CBeebies, which is directed to children under 6 years old. The website content is specifically tailored for respective age groups.

Good practice: Policy and technology

Twitter has continuously invested in proprietary technology, which has contributed to steadily reducing the burden on people to report.[1] Specifically, more than 50 per cent of Tweets, compared with 20 per cent in 2018, that Twitter follows up in response to their abusive nature, are currently proactively surfaced using technology, rather than relying on reports to Twitter. The new technology is used to deal with the policy content areas of private information, sensitive media, hateful conduct, abuse and impersonation.

[1] Twitter, "15th Transparency Report: Increase in proactive enforcement on accounts".

3.2 Developing standard processes to handle CSAM

In 2019, IWF actioned 132,676 webpages confirmed as containing child sexual abuse.[13] 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.

[13] IWF, "The why. The how. The who. And the results. Annual Report 2019".

While many governments are tackling the dissemination and distribution of CSAM by enacting legislation, pursuing and prosecuting abusers, raising awareness, and supporting children and young people in recovering from abuse or exploitation, there are many countries that do not yet have adequate systems in place. Mechanisms are required in each country to enable the general public to report abusive and exploitative content of this nature. Industry, law enforcement, governments and civil society must work together to ensure that adequate legal frameworks in accordance with international standards are in place. Such frameworks should criminalize all forms of CSEA, including through CSAM, and protect children who are victims of such abuse or exploitation. These frameworks must ensure that reporting, investigations and content removal processes work as efficiently as possible.

Industry should provide links to national hotlines or other locally available hotlines, such as IWF portals in some countries and, in the absence of local reporting opportunities, provide links to other international hotlines as relevant, such as the United States National Center for Missing and Exploited Children (NCMEC) or the International Association of Internet Hotlines (INHOPE), where any of the international hotlines can be used to file a report.

Responsible companies are taking a number of steps to help prevent their networks and services from being used to disseminate CSAM. These include introducing language into terms and conditions or codes of conduct that explicitly forbids such content or conduct;[14] developing robust notice and takedown processes; and working with and supporting national hotlines.

Additionally, some companies deploy technical measures to prevent the misuse of their services or networks for sharing known CSAM. For example, some Internet service providers are blocking access to URLs confirmed by an appropriate authority as containing CSAM if the website is hosted in a country where processes are not in place to ensure it will be rapidly taken down. Others are deploying hashing technologies to automatically detect and remove images of child sexual abuse that are already known to law enforcement or hotlines. Industry members should consider and incorporate all relevant services for their operations to prevent the dissemination of child sexual abuse.

Industry actors should commit to allocate proportionate resources and continue to develop and share preferably open source technological solutions to detect and remove CSAM.

Good practice: Technology

Microsoft uses a four-pronged approach to foster responsible and safe technology use, with a focus on the technology itself, self-governance, partnerships, and consumer education and outreach. Microsoft has also embedded features that help empower individuals to more effectively manage their online safety. "Family Safety" is one such feature, which permits parents and carers to monitor their children's Internet use.

Microsoft enforces policies against harassment on its platforms, and users who abuse these regulations are subject to account termination or, in case of more serious violations, to law enforcement measures.

[14] It should be noted that inappropriate user conduct is not limited to CSAM and that any type of inappropriate behaviour or content should be handled accordingly by the company.

Microsoft PhotoDNA is a tool that creates hashes of images and compares them to a database of hashes already identified and confirmed to be CSAM. If it finds a match, the image is blocked. This tool has enabled content providers to remove millions of illegal photographs from the Internet; helped convict child sexual predators; and in some cases, helped law enforcement rescue potential victims before they were physically harmed. Microsoft has long been committed to protecting its customers from illegal content on its products and services, and applying technology the company already created to combating this growth in illegal videos was a logical next step. However, this tool does not employ facial recognition technology, nor can it identify a person or object in the image. However, with the invention of PhotoDNA for Video, things have taken a new turn. PhotoDNA for Video breaks down a video into key frames and essentially creates hashes for those screenshots. In the same way that PhotoDNA can match an image that has been altered to avoid detection, PhotoDNA for Video can find child sexual exploitation content that has been edited or spliced into a video that might otherwise appear harmless.

Moreover, Microsoft has recently released a new tool for identifying child predators who groom children for abuse in online chats. Project Artemis, developed in collaboration with The Meet Group, Roblox, Kik and Thorn, builds on Microsoft's patented technology and will be made freely available via Thorn to qualified online service companies that offer a chat function. Project Artemis is a tech tool which helps to raise red flags to administrators when moderation is needed in chat rooms. With this grooming detection technique, it will be possible to identify, address and report predators attempting to lure children for sexual purposes.

The **IWF** provides a range of services to industry members to protect their users from stumbling across CSAM. These include:

- A dynamic, quality-assured URL blocking list of live material;
- A hash list of known criminal content related to CSAM;
- A unique keyword list of cryptic terms known to be associated with CSAM;
- A list of details of domain names that are known for hosting child sexual abuse content to enable the rapid removal of domains hosting illegal content.

3.3 Creating a safer and age-appropriate online environment

Very few things in life can be considered absolutely safe and risk-free all of the time. Even in cities where the movement of traffic is highly regulated and closely controlled, accidents still happen. By the same token, cyberspace is not without risks, especially for children and young people. 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:[15]

[15] Sonia Livingstone et al., "EU Kids Online: Final Report", London school of economics, 2009.

- *Inappropriate content* – Children and young people may stumble upon inappropriate and illegal content while searching for something else by clicking a presumably innocuous link in an instant message, on a blog or when sharing files. They may also seek out and share inappropriate or age-sensitive material. What is considered harmful content varies from country to country; examples include content that promotes substance abuse, racial hatred, risk-taking behaviour, suicide, anorexia or violence.
- *Inappropriate conduct* – Children and adults may use the Internet to harass or even exploit other people. Children may sometimes broadcast hurtful comments or embarrassing images or may steal content or infringe on copyrights.
- *Inappropriate contact* – Both adults and young people can use the Internet to seek out children or other young people who are vulnerable. Frequently, their goal is to convince the target that they have developed a meaningful relationship, but the underlying purpose is manipulative. They may seek to persuade the child to perform sexual or other abusive acts online, using a webcam or other recording device, or they will try to arrange an in-person meeting and physical contact. This process is often referred to as "grooming".
- *Commercial risks* – This category refers to data privacy risks related to the collection and use of children's data, as well as digital marketing. 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 by design and age-appropriate for their broad range of users. Additional approaches include offering tools to develop appropriate age-verification systems that respects children's rights to privacy and access or place restrictions on children and young people's access to age-inappropriate content, or restrict the people with whom children might have contact or the times at which they may go online. Most importantly, "safety by design"[16] frameworks including privacy need to be incorporated into innovation and product design processes. Children's safety and responsible use of technology has to be carefully considered and not be an afterthought.

Some programmes allow parents to monitor the texts and other communications that their children and young people send and receive. If programmes of this type are to be used, it is important that this is discussed openly with the child, otherwise such conduct can be perceived as "spying" and may undermine trust within the family.

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 and transparent reporting mechanisms should be made available to users who have concerns about content and behaviour. Furthermore, reporting needs to be followed up appropriately, with timely provision of information about the status of the report. Although companies can vary their implementation of follow-up mechanisms on a case-by-case basis, it is essential to set a clear time frame for responses, communicate the decision made regarding the report, and offer a method for following up if the user is not satisfied with the response.

[16] eSafety Commissioner, Safety by Design Overview, 2019.

Good practice: Reporting

Facebook, in an effort to curb sexual harassment on digital platforms, has co-financed Project deSHAME with the European Union, a collaboration among Childnet, Save the Children, Kek Vonal and UCLan. This project aims to increase reporting of online sexual harassment among minors and improve multisector cooperation in preventing and responding to this behaviour.

As one main purpose of the project is to encourage users to report content that is upsetting or inappropriate, Facebook's Community Standards are also relevant as guidelines on what is and is not allowed on Facebook. They also outline the types of users that it does not allow to post. Facebook has also created safety features such as the "Do you know this person?" feature; an "other" inbox gathering new messages from people the user does not know; and a popup which appears on the news feed if it looks like a minor is being contacted by an adult that they do not know.

Online content and service providers can also describe the nature of content or services they are providing and the intended target age range. These descriptions should be aligned with pre-existing national and international standards, relevant regulations, and advice on marketing and advertising to children made available by the appropriate classification bodies. This process becomes more difficult, however, with the growing range of interactive services that enable the publication of user-generated content, for example, via message boards, chat rooms and social networking services. When companies specifically target children and young people, and when services are overwhelmingly aimed at younger audiences, the expectations **in user-friendly, easily understandable and accessible terms of content** and security will be much higher.

Companies are also encouraged to adopt the highest privacy standards when it comes to collecting, processing and storing data from or about children and young people, as children and young people may lack the maturity to appreciate the wider social and personal consequences of revealing or agreeing to share their personal information online, or to the use of their personal information for commercial purposes. Services directed at or likely to attract a main audience of children and young people must consider the risks posed to them by access to, or collection and use of, personal information (including location information), and ensure those risks are properly addressed, and users informed. In particular, companies should ensure the language and style of any materials or communication used to promote services, provide access to services, or by which personal information is accessed, collected and used, aid understanding and assist users in managing their privacy in clear and simple ways, and explaining what they are consenting to in clear, accessible language.

Good practice: Innovation

In 2018 –2019 UNICEF East Asia and Pacific Regional Office organized five multi-stakeholder roundtables to share promising industry practices to address online CSEA. Participants in the roundtables were leading private sector companies, such as Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Mongolia) Mobifone+ (Vietnam), Globe Telecom (the Philippines), True (Thailand), GSMA and civil society partners, including INHOPE, ECPAT International and Child Helpline International.

As part of the same project, in February 2020, UNICEF launched a Think Tank to accelerate industry leadership in the East Asia and Pacific region to prevent violence against children in the online world. The Think Tank is an incubator for ideas and innovation, drawing on the unique perspective of industry actors (product creation, marketing, etc.) for the development of impactful educational materials and identification of the most effective delivery platforms, as well as for the development of an evaluation framework that can measure the impact of these educational materials and messages targeted at children. The Think Tank is comprised of Facebook, Telenor, academic experts, United Nations agencies, such as ITU, UNESCO and UNODC, and others, such as the Australia eSafety Commissioner, ECPAT International, ICMEC, INTERPOL, and the End Violence Global Fund. The Think Tank inaugural meeting, held in parallel to the ASEAN Regional Conference on Child Online Protection, drew together experts, including Microsoft, to explore technology and research possibilities for better tracking changes in online behaviour, based on uptake of online safety materials and messages.

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

Technical measures can be an important part of ensuring that children and young people are protected from the potential risks online, but these are only one element of the equation. **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.

Many companies are investing in educational programmes designed to enable users to make informed decisions about content and services. Companies are assisting parents, caregivers and educators in guiding children and young people towards safer, more responsible and appropriate online and mobile phone experiences. This includes sign posting age-sensitive content and ensuring that information on items such as content prices, subscription terms and how to cancel subscriptions, is clearly communicated. Promoting respect of the minimum age requirement by social media in all countries where age verification is possible would also help to protect children by allowing them to access services at an appropriate age. An important consideration that needs to go alongside this recommendation is the additional personal data collection that this may entail and the need to limit the collection and storage of this information and its processing.

It is also important to provide information directly to children and young people on safer ICT use and positive and responsible behaviour. Beyond raising awareness about safety, companies can facilitate positive experiences by developing content for children and young people about being respectful, kind and open-minded when using ICTs and looking after friends. They can provide information about actions to take if they have negative experiences such as online bullying or grooming, making it easier to report such incidents and providing a function to opt out of receiving anonymous messages.

Parents sometimes have less understanding and knowledge of the Internet and mobile devices than children and young people. Moreover, the convergence of mobile devices and Internet services makes parental oversight more difficult. 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. The aim is not to transfer responsibility for children and young people's ICT use to parents alone, but rather to recognize that parents are in a better position to decide what is appropriate for their children and that they should be made aware of all risks in order to better protect their children and empower them to take action.

Information can be transmitted online and offline through multiple media channels, taking into consideration that some parents do not use Internet services. It is important to collaborate with school districts to provide curricula on online safety and responsible ICT use for children and young people, and educational materials for parents. Examples include explaining the types of services and options available for monitoring activities, actions to take if a child is experiencing online bullying or grooming, how to avoid spam and manage privacy settings, and how to talk with boys and girls of different age groups about sensitive issues. Communication is a two-way process and many companies provide options for customers to contact them to report issues or discuss concerns.

As content and services grow ever richer, all users will continue to benefit from advice and reminders about the nature of a particular service and how to enjoy it safely. While it is important to teach children about responsible use of the Internet, we know children like to experiment, take risks, are inherently curious and may not always make the best decisions. Giving them the chance to exercise their agency contributes to their growth and is a healthy way to help them develop autonomy and resilience, as long as the blowback is not too harsh. 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.

Good practice: Education

NHK Japan runs a suicide prevention campaign for young people on Twitter: In Japan, suicides among teenagers peak when they go back to school after a summer vacation. The return to reality is said to be the reason for the peak. The NHK Heart Net TV (NHK Japan) production team produces a multimedia programme #On the Night of August 31st. Linking television, live streaming, and social media, NKH successfully created a "place" where teenagers could share their feelings without fear.

Good practice: Education

Twitter has also published a guide for educators on media literacy. Drawn up with UNESCO, the handbook primarily aims to help educators equip younger generations with media literacy skills. Another aspect of Twitter's safety work relates to their disclosure of information operations. This is an archive of State-backed information operations, which Twitter shares publicly. The initiative was launched to empower academic and public understanding of the campaigns related to this issue around the world, and to empower independent, third-party scrutiny of these tactics on the Twitter platform.

Project deSHAME, co-financed by Facebook and the European Union, also facilitates the creation of resources for a wide range of age groups, with a particular focus on children aged 9–13 years. As part of the project, a toolkit called "Step Up, Speak Up!" has been developed, providing a range of education, training and awareness-raising materials, as well as practical tools for multisector prevention and response strategies. The project will transfer these learning materials to other European countries and partners worldwide in order to promote young people's digital rights.

Google has developed an array of educational initiatives, resources and tools to help promote online safety for youth. One of them is the Be Internet Awesome campaign around digital citizenship, created in collaboration with organizations such as ConnectSafely, the Family Online Safety Institute and the Internet Keep Safe Coalition. This campaign is targeted towards young people aged 8–11 years. It features a web-based game for youth (Interland) that teaches digital safety fundamentals and resources for educators, such as Digital Citizenship and Safety Curriculum. The Safety Curriculum offers lesson plans for the campaign's five key thematic areas, one of which focuses on cyberbullying. In addition to this, Google has generated an online digital citizenship and safety course for educators of students of all ages, providing further support for integrating digital citizenship and activities on safety in the classroom. Google also offers several programmes to help engage young people directly in online safety and digital citizenship efforts. The global Web Rangers initiative is one such programme that teaches young people about online safety and encourages them to design their own campaigns around positive and safe Internet use. There are also country-specific programmes for young people, such as the Internet Citizens and Internet Legends programmes in the United Kingdom, launched by Google.

In the **Eurovision Youth News Exchange**, the European Broadcasting Union gathers 15 European television broadcasters to share programmes, formats and solutions online and offline. In recent years, teaching digital literacy and alerting children to risks on the Internet have become central to their programmes. Among the most successful initiatives of recent years are the social media ads and news programmes suitable for children produced by Super and Ultra nytt under NRK, Norway's public broadcaster.

Good practice: Strategic partnerships

As part of a project supported by the End Violence Against Children Fund, in 2018 Capital Humano y Social Alternativo entered into a partnership with Telefónica, the largest Internet, cable and telephone service provider in Peru, with 14.4 million customers, including more than 8 million Movistar mobile users.

Several activities were carried out under this fruitful partnership:

- **A virtual course on child online protection** was developed by Telefónica with the technical support of Capital Humano y Social Alternativo. This course is now openly available on Telefónica's website and the company is tracking the number of people who enroll and successfully complete the course. The Peruvian Ministry of Education agreed to include access to this virtual course through its official website.
- **A booklet on Internet safety** was created by Capital Humano y Social Alternativo and distributed by Telefónica in its over 300 mobile sales centres. The aim is to raise awareness among Telefónica customers of online safety and the risks associated with online CSEA.
- **An interactive game on online CSEA** was developed by Telefónica with the technical support of Capital Humano y Social Alternativo, which its customers can play while waiting for their turns at Telefónica's stores.

Building on the success with Telefónica, Capital Humano y Social Alternativo partnered with **Econocable**, an Internet and cable service provider that works in remote and low-income areas in Peru.

3.5 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. It is essential to ensure that age verification systems do not jeopardize the genuine need for specific age groups to access content that is relevant for their development.

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. They can emphasize the Internet's capacity to facilitate positive engagement in broader civic life, drive social progress, and influence the sustainability and resilience of communities, for example, by participating in social and environmental campaigns and holding those in charge accountable. With the right tools and information, children and young people are better placed to access opportunities for health care, education and employment, and to voice their opinions and needs in schools, communities and countries. They become empowered to access information about their rights and seek information about matters that affect them personally, such as their sexual health, 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. They should always consider safety by design in their products.

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 – the ability to understand and interact in the digital world. Without this ability, citizens are not able to participate in many of the social functions that have become digitized, including filing taxes, supporting political candidates, signing online petitions, registering a birth, or simply accessing commercial, health, educational or cultural information. Without action, the gap between citizens who are able to access these forums and those who are not, due to a lack of Internet access or digital literacy, will continue to widen, placing the latter at a significant disadvantage. Companies can support multimedia initiatives to foster the digital skills that children and young people need to be confident, connected and actively involved citizens.[17] In many countries, digital and media literacy, and efforts to close the digital divide have been part of the mission of the public service media over recent years. The Italian Parliament, for example, has proposed that the national broadcaster's priorities include closing the digital divide and ensuring child protection both offline and online, an example which could be followed by other countries.

[17] For examples of youth participation from the mobile community see here.

Good practice: Multiagency collaboration

Recently, Microsoft joined the global campaign Power of ZERO, led by the organization No Bully, which aims to help young children, and the adults who care for them, learn to use digital technology well and develop the voice, compassion and inclusivity that are the heart of digital citizenship. The initiative offers early educators (the campaign is targeted towards children ages 8 and under) and families with free learning materials to help young children cultivate the "12 powers for good" (Power of Zero's 12 life skills or "powers," for children to successfully navigate both the online and offline world, including resilience, respect, inclusivity and creativity) and lay a strong foundation for them at an early age.

4. General guidelines for industry

Table 1 outlines broad guidelines 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.

Note that not all the steps listed in Table 1 will be appropriate across all companies and services, and nor are all the necessary steps for each service found in this Table. The general guidelines for industry are complemented by the feature-specific checklists (see section 5) and vice-versa. The feature-specific checklists in Tables 2–5 highlight additional steps that are most relevant for individual services. Note that the feature-specific checklists may overlap, and that more than one checklist can be relevant for the same service.

Table 1: General guidelines for industry

Integrating child rights considerations into all appropriate corporate policies and management processes	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:
	Ensure that a specific individual and/or team is designated with responsibility for this process and has access to the necessary internal and external stakeholders. Authorize this person or team to take the lead in raising the profile of child online protection across the company.
	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).
	Integrate due diligence on COP issues into existing human rights or risk assessment frameworks (at the corporate, product or technology and/or country level) to determine whether the business or industry may be causing or contributing to adverse impacts through its activities, or whether adverse impacts may be directly attributed to its operations, products or services, or business relationships.
	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.

Integrating child rights considerations into all appropriate corporate policies and management processes (*cont.*)	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. Draw upon internal and external expertise and consult with key stakeholders, including children and young people, on child online safety mechanisms to obtain ongoing feedback and guidance on company approaches.
	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.
	Ensure access to remedy by establishing operational-level grievance and reporting mechanisms for any child rights violations (e.g. CSAM, inappropriate content or contact or breaches of privacy).
	Nominate a child protection policy manager or other designated person who can be contacted for COP issues. If a child is at risk of harm, the child protection policy manager should immediately alert the appropriate authorities. The BBC editorial guidelines (2019), for example, specify the appointment of a child protection policy manager, which is considered mandatory within public service media.
Developing industry standards to protect children online	Create and implement company and industry standards for the protection of children and young people, with regard to the specific industry and features.
Developing standard processes to CSAM	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. Where a company is operating in markets with less developed regulatory and law enforcement oversight of this issue, it can refer those wishing to file reports to the International Association of Internet Hotlines (INHOPE), where reports can be filed with any international hotline.

Developing standard processes to CSAM (***cont.***)	Establish internal procedures to ensure compliance under local and international laws on combating CSAM. Establish a senior position or team dedicated to integrating these procedures into the organization. Industry members should then report the actions taken and outcomes achieved by this team in their annual corporate and sustainability report. When national regulations do not provide sufficient protection, companies should respect but exceed national legislation and use their leverage to lobby for legislative changes to enable industry to combat CSAM. A senior position or team should be created within the organization, dedicated to integrating these procedures and monitoring the operations. These should be transparently reflected in the annual corporate and sustainability reports and made available to the public.
	Specify that the business will cooperate fully with law enforcement investigations in the event that illegal content is reported or discovered and note details regarding such penalties as fines or cancellation of billing privileges.
	Use customer terms and conditions and/or acceptable use policies to explicitly state the company's position on the misuse of its services to store or share CSAM and the consequences of any abuse.
	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. Establish report follow-up processes, agree on procedures to capture evidence and immediately remove or block access to CSAM. Ensure that, where needed, service providers request the opinion of experts (e.g. national COP bodies) before destroying illegal content. Ensure that relevant third parties with whom the company has a contractual relationship have similarly robust notice and take down processes in place.
	Be prepared to handle CSAM and report cases to the appropriate authorities. If a relationship with law enforcement and the national hotline is not already established, engage with them to develop processes together.
	Work with internal functions, such as customer care, fraud prevention and security to ensure that the business can submit reports of suspected illegal content directly to law enforcement and hotlines. Ideally, this should be done in a way that neither exposes front-line staff to harmful content nor re-victimizes the affected child/children and young people. To address situations where staff may be exposed to abusive material, implement a policy or programme to support staff resiliency, safety and well-being.

Developing standard processes to CSAM (*cont.*)	Include data retention and preservation policies to support law enforcement in the event of criminal investigations through such activities as capturing evidence. Document the company's practices for handling CSAM, beginning with monitoring and extending to the final transfer and destruction of the content. Include a list of all personnel responsible for handling the material in the documentation.
	Promote reporting mechanisms for CSAM and ensure that customers know how to file a report if they discover such content. If a national hotline is available, offer links to that hotline from the corporate website and from any relevant content services promoted by the company.
	Take all relevant services/data sets to prevent the dissemination of known child sexual abuse content on their services or platforms.
	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.
Creating a safer and age-appropriate online environment	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 company 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. In addition to the age-appropriate and accessible terms and conditions, industry should similarly, and clearly communicate information, such as rules and key policies. This should emphasize acceptable and unacceptable behaviour on the service, the consequences of breaking any rules, the specifics of the service and what the user is consenting to through signing up. Such information should be particularly geared towards young users and their parents and caregivers.
	Use terms of service or terms and conditions to draw users' attention to content in the company's online services that may not be appropriate for all ages. The terms and conditions should also include clear mechanisms for reporting and dealing with infringements of such rules.

Creating a safer and age-appropriate online environment (*cont.*)	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. These include block/allow lists, content filters, usage monitoring, contact management and time/programme limits.
	Offer easy-to-use parental control options that allow parents and carers to restrict certain services and content that children can access when using electronic devices. These restrictions can include network and device level controls, and application controls. Considering that this has huge implication on a child's ability to advance their digital skills and impair their opportunities online, these controls should be designed for very young children in line with their developmental context and with appropriate guidance for parents.
	Where possible, promote national support services that parents and caregivers may use to report infringements and seek support in the case of abuse or exploitation.
	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. Harmful advertising can also include advertising of food and drinks that are high in fat, sugar or salt. Align business practices with regulations and advice on marketing and advertising to children and young people. Monitor where, when and how children and young people might encounter potentially harmful advertising messages intended for another market segment.
	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.
	Adapt and implement heightened default privacy settings for collection, processing, storage, sale and publishing of personal data, including location-related information and browsing habits, gathered from people under 18 years. Default privacy settings and information about the importance of privacy should be appropriate to the age of the users and the nature of the service.
	Employ technical measures, such as appropriate parental control tools, safety by design, age-differentiated experiences, password-protected content, block/allow lists, purchase/time controls, opt-out functions, filtering and moderating, to prevent underage access and exposure to inappropriate content or services. Implement technology that can identify the age of users and present them with a version of the application that is age appropriate. For age-sensitive content or services, industry stakeholders should take steps to verify users' ages. Where possible, use age verification to limit access to content or material that, either by law or policy, is intended only for persons above a certain age. Companies should also recognize the potential for misuse of such technologies to restrict children and young people's right to freedom of expression and access to information or endanger their privacy.

Creating a safer and age-appropriate online environment ***(cont.)***	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. For example, with regard to media standards, all media regulatory authorities provide a set of requirements for age-related content and Internet providers are required to adapt the repositories and apply the guidelines to their content offer. See, Ofcom in the United Kingdom, CSA in France and AGCOM in Italy.
	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 rights to privacy and their evolving capacities. Active moderation can encourage an atmosphere where bullying and harassment are not acceptable. Unacceptable behaviour includes: • posting unpleasant or threatening comments on someone's profile; • setting up fake profiles or hate sites to humiliate a victim; • sending chain messages and attachments with harmful intent; • hacking into someone's account to send offensive messages to others.
	Take special precaution with staff members or collaborators who work with children and young people, for whom a preliminary criminal record check with police authorities may be required.
	Refer any incident of suspected grooming promptly to the online or interactive executive management team responsible for reporting it to the appropriate authorities: • report grooming to the executive management team and to a nominated child protection policy manager, where possible; • enable users to report suspected grooming incidents directly to the authorities; • establish the possibility for direct contact through email addresses to alert and report.
	Prioritize the safety and well-being of the child at all times. Always act within professional boundaries and ensure all contact with children is essential to the service, programme, event, activity or project. Never take sole responsibility for a child. If a child needs care, alert the parent, guardian or chaperone. Listen to and respect children at all times. If anyone is behaving inappropriately around children, report the behaviour to the local child protection contact.

Creating a safer and age-appropriate online environment (*cont.*)	Establish a clear set of rules that are prominently placed and echo key points from the terms of service and acceptable use guidelines. User-friendly language for these rules should define: • the nature of the service and what is expected of its users; • what is and is not acceptable in terms of content, behaviour and language, as well as prohibiting illegal usage; • the consequences proportionate to the breach, for example, reporting to law enforcement or suspension of the user's account.
	Make it easy for customers to report concerns about misuse to customer care, with standard and accessible processes in place to deal with different concerns, such as receiving unwanted communications (e.g. spam SMS).
	Be transparent and provide customers with clear information about the nature of the services offered, for example: • type of content/service and costs; • minimum age required for access; • availability of parental controls, including what the controls cover (e.g. network) or do not cover (e.g. Wi-Fi) and training on how to use them; • type of user information collected and how it is used.
	Promote national support services that enable children and young people to report and seek support in the case of abuse or exploitation (see, for example, Child Helpline International).
Educating children, parents and educators about children's safety and their responsible use of ICTs	Industry can complement technical measures with educational and empowerment activities by taking the following actions:
	Clearly describe available content and corresponding parental controls or family safety settings. Make language and terminology accessible, visible, clear and relevant for all users, including children, parents and caregivers, especially in relation to terms and conditions, costs involved in using content or services, privacy policies, safety information and reporting mechanisms.
	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.
	Set up mechanisms and educate parents to become involved in their children and young people's ICT activities, particularly those of younger children, by, for example, enabling parents to review children and young people's privacy settings.
	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.

Educating children, parents and educators about children's safety and their responsible use of ICTs (*cont.*)	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.
	Support customers by disseminating guidelines on family online safety that encourage parents and caregivers to: • familiarize themselves with products and services used by children and young people; • ensure moderate use of electronic devices by children and young people as part of a healthy and balanced lifestyle; • pay close attention to children and young people's behaviour in order to identify changes that could indicate cyberbullying or harassment.
	Provide parents with the necessary information to understand how their children and young people are using ICT services, handle issues related to harmful content and conduct and be equipped to guide children and young people in responsible usage. This can be facilitated through the use of tools and interactions with school districts to provide online safety curricula for children and educational materials for parents.
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.
	Public service and national media can play an essential role through their programme offers (offline and online) to educate parents and children and make them aware of the risks and opportunities of the online world
Promoting digital technology as a mode to further civic engagement	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.

Promoting digital technology as a mode to further civic engagement (***cont.***)	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. This process should be available to all consumers, including webmasters. Any reporting process should provide clear, responsible and adjudicated terms of service.
	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.
	Develop educational content for children and young people that encourages learning, creative thinking and problem solving.
	Promote digital literacy, capacity building and ICT skills to equip children and young people, particularly those in rural and underserved areas, to utilize ICT resources and fully participate safely in the digital world.
	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.
	Inform and engage customers, including parents, caregivers, children and young people, about the services ⁋ offered, for example: • type of content and corresponding parental controls; • reporting mechanisms for cases of abuse, misuse and inappropriate or illegal content; • follow-up procedures for reports; • types of services that are age restricted; • safe and responsible use of "own-brand" interactive services.
	Engage with the broader issues around safe and responsible digital citizenship, for example online reputation and digital footprint, harmful content and grooming. Consider partnering with local experts, such as children's NGOs, charities and parenting groups, to help shape the company's message and reach the intended audience.
	If the business already works with children or schools, for example, through ⁋ corporate social responsibility programmes, investigate the possibility of extending this engagement to include educating and engaging with children and young people, and **educators** on COP messages.
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 and better understand what types of interventions are most effective at improving children's online experiences.

Typology of ICT companies

While these ITU guidelines are targeted at the ICT industry as a whole, it is important to recognize that the services ICT companies offer, ways they operate, regulatory schemes under which they function, and scope and scale of their offers are very different. Any technology company whose products and services are targeted directly or indirectly at children can benefit from the general principles outlined earlier and can adapt, based on their specific field of operation. The core idea is to support and guide the ICT industry in taking the right measures to better protect children online from the risks of harm while empowering them to navigate the online world in the best way possible. The typology below will help provide a clearer understanding of some of the target audiences and how they fit in the checklists in the following section. It should be noted that these are only some specific example categories and are not exhaustive:

(a) Internet service providers, including through fixed landline broadband services or cellular data services of mobile network operators: while this typically reflects services offered over a more long-term basis to subscribed customers, it could also be extended to businesses that provide free or paid public WI-FI hotspots.
(b) Social network /messaging platforms and online gaming platforms.
(c) Hardware and software manufacturers, such as providers of handheld devices including mobile phones, gaming consoles, voice assistance-based home devices, Internet of Things and smart Internet connected toys for children.
(d) Companies providing digital media (content creators, providing access to or hosting content).
(e) Companies providing streaming services, including live streams.
(f) Companies offering digital file storage services, cloud-based service providers.

5. Feature-specific checklists

This chapter complements the previous general checklist for industry by offering recommendations for businesses that provide services with specific features on respecting and supporting children's rights online. The following feature-specific checklists outline ways to supplement the common principles and approaches presented in Table 1, as they apply to different services, and should therefore be considered in addition to the steps in Table 1.

The features highlighted here are crosscutting and several feature-specific checklists may be relevant for the same company.

The following feature checklists are organized by and refer back to the same key areas as the general guidelines in Table 1. Each of the feature checklists has been developed in collaboration with key contributors and, as a result, there are minor variations in the tables.

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

Mobile operators enable access to the Internet and offer a range of mobile-specific data services. Many operators have already signed up to COP codes of practice and offer a range of tools and information resources to support their commitments.

Most Internet service providers act 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.

Internet access in public spaces

It is becoming increasingly common for municipalities, retailers, transportation companies, hotel chains and other businesses and organizations to provide Internet access via Wi-Fi hotspots. Such access is typically free or provided at minimal cost, and sometimes with minimal sign-on formalities as a public service, or by a company to attract customers to its premises or persuade more people to use its services.

Promoting Wi-Fi is an effective way to ensure Internet availability in a given area. Care needs to be taken, however, when such access is provided in public spaces where children are likely to be present on a regular basis. Users need to be mindful of the fact that Wi-Fi signals might be available to passers-by and user data compromised. The Wi-Fi provider will therefore not always be able to support or supervise the use of an Internet connection it has supplied and users need to therefore take precautions not to share sensitive information over publicly available Wi-Fi.

In public spaces, Wi-Fi providers may want to consider additional measures to protect children and young people, such as:

- Proactively blocking access to web addresses known to contain content that is inappropriate for a wide audience, in addition to their efforts to blocking access to CSAM.
- Including clauses in terms and conditions of use that forbid the use of Wi-Fi services to access or display any material that may be unsuitable in an environment where children are present. The terms and conditions should also include clear mechanisms regarding the consequences of infringements of such rules.
- Taking all measures to protect against unauthorized access, which may result in manipulation or loss of personal data.
- Installing filters on the Wi-Fi system to reinforce the policy on inappropriate material.
- Providing procedures and software to signpost and offer optional parental control related to children and young people's access to Internet content.

Good practice: The telecommunication regulations of most European Union member states, for example, stipulate that access to the network must be identified, through individual SIM cards or other identification tools.

Table 2 provides guidance for providers of connectivity, data storage and hosting services on actions they can take to enhance child online protection and children's participation.

Table 2: COP checklist for Feature A: Provide connectivity, data and hosting devices

Integrating child rights considerations into all appropriate corporate policies and management processes	Providers of connectivity, data storage and hosting services 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.
	Refer to the general guidelines in Table 1.
Developing standard processes to handle CSAM	In collaboration with government, law enforcement, civil society and hotline organizations, providers of connectivity, data storage and hosting services can play a key role in combating CSAM by taking the following actions:
	Collaborate with government, law enforcement, civil society and hotline organizations to effectively handle CSAM and report cases to the appropriate authorities. If a relationship with law enforcement and a hotline is not already established, engage with them to develop processes together. Providers of connectivity, data storage or hosting services may also provide ICT training for law enforcement. If a company is operating in markets with less developed legal and law enforcement oversight of this issue, it can refer those wishing to file reports to the International Association of Internet Hotlines (INHOPE) where reports can be filed with any international hotline.
	Consider deploying internationally recognized URL or website blocking lists created by appropriate authorities (e.g. the national law enforcement or hotline, Cybertip Canada, Interpol, IWF), to make it harder for users to access identified CSAM.
	Develop notice and take down and reporting processes, and link reports of abuse to those processes with a public service agreement on the response procedure and takedown times. See, for example, the UNICEF and GSMA Guide on notice and takedown policies and practices.
	Set up a reporting mechanism with clear information on its usage by, for example, giving guidance on the illegal content and conduct to be reported and clarifying what materials cannot be attached with the report in order to avoid further distribution on the web.

Developing standard processes to handle CSAM (*cont.*)	Support law enforcement in the event of criminal investigations through such activities as capturing evidence. Use terms of service and conditions to specifically prohibit the use of services to store, share or distribute CSAM. Make sure these terms clearly state that CSAM will not be tolerated. Make sure that terms of service and conditions state that the company will cooperate fully with law enforcement investigations in the event CSAM is discovered or reported.
	There are currently two reporting solutions for CSAM online at the national level: hotlines and reporting portals. A full up-to-date list of all existing hotlines and portals can be found at INHOPE. Hotlines: If a national hotline is not available, explore opportunities to set one up (see the GSMA INHOPE Hotlines Guide for a range of options, including working with INHOPE and the INHOPE Foundation. An interactive version of the GSMA INHOPE guide is available that provides guidance on how to develop internal processes for customer care staff to submit reports of questionable content to law enforcement and INHOPE. Reporting portals: The IWF offers a reporting portal solution that allows Internet users in countries and nations without hotlines, to report images and videos of suspected child sexual abuse directly to the IWF through a bespoke online portal page.
	For providers of connectivity, data storage and hosting services whose services involve some kind of content hosting (many do not), notice and take down processes should be in place.
Creating a safer and age-appropriate digital environment	Providers of connectivity, data storage and hosting services, can help create a safer, more enjoyable digital environment for children of all ages by taking the following actions:
	Data storage / hosting service providers should consider presenting the reporting function on all web pages and services, and develop and document clear processes for swiftly managing reports of abuse or other breaches of terms and conditions.
	Providers of connectivity should offer own-brand technical controls or signpost the availability of tools created by specialist providers that are appropriate for the services offered and are easy for end users to implement and offer the possibility of blocking or filtering access to the Internet through the company networks. Provide appropriate age-verification mechanisms if the company offers content or services (including own brand or third-party services that are promoted by the company), that are only legal or appropriate for adult users (e.g. certain games, lotteries).

Educating children, parents and educators about children's safety and their responsible use of ICTs	Providers of connectivity, data storage and hosting services should echo key messages from terms and conditions within community guidelines written in user-friendly language to support children and their parents and caregivers. Within the service itself, at the point of uploading content, include reminders about such topics as the type of content considered to be inappropriate.
	Provide children and young people with information on safer Internet use. Consider creative ways to promote key messages such as the following: "Never share any contact details, including your physical location and your phone number, with anyone you don't know in person." "Never agree to get together with anyone you have met online on your own without consulting an adult first. Always tell a trusted friend about your whereabouts." "Do not respond to bullying, obscene or offensive messages. But save the evidence – do not delete the message." "Tell a trusted adult or friend if you are uncomfortable or upset about something or someone." "Never give away your account password or username! Be aware that other people online may give false information to convince you to share your private information."
	Service providers can partner with organizations that are well-positioned to educate and support children on safer internet usage and related issues. See Child Helpline International and GSMA practical guide for Child Helplines and Mobile Operators: Working together to protect children's rights for examples.
Promoting digital technology as a mode to further civic engagement	*Refer to the general guidelines in Table 1.*

5.2 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.

Table 3 provides guidance for providers of services offering editorially curated content on policies and actions they can take to enhance child online protection and participation.

Table 3: COP checklist for Feature B: Offer curated digital content

Integrating child rights considerations into all appropriate corporate policies and management processes	Services providing curated digital content can help identify, prevent and mitigate 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 policies that safeguard the welfare of children and young people who contribute content online to take into account the physical and emotional welfare and dignity of people under 18 who are involved in programmes, films, games, news etc. irrespective of consent that might have been given by a parent or other adult.
Developing standard processes to handle CSAM	In collaboration with government, law enforcement, civil society and hotline organizations, companies offering curated digital content can play a key role in combating CSAM through the following actions: In cases of CSAM, for example through "comment" or "review" features whereby users have the capacity to upload content, staff should contact the executive management team responsible for reporting such material to the appropriate authorities. In addition, they should: • alert national law enforcement agencies immediately; • alert their manager and report the material to the child protection policy manager; • contact the internal investigation service by phone or email with details of the incident and to ask for advice; • wait for advice from the relevant agency before deleting the material, saving it to a shared space or forwarding it.

Developing standard processes to handle CSAM	If the material is identified, it should be reported directly to an organization specialized in Internet safety that operates a hotline reporting system for members of the public and information technology professionals to report specific forms of potentially illegal online content. For example, based on its Child Protection and Safeguarding Policy, the BBC has released editorial guidance on interacting with children and young people online. It has developed further checklists and codes of conduct for working with children and young people online, which also extend to the subcontractors and external providers. Ofcom's policy on child protection for the United Kingdom addresses online content, mobile devices and game consoles separately. Implement a swift and robust escalation strategy if CSAM is posted or illegal conduct is suspected. To this end: • offer users a simple and easily accessible method of alerting the content producer to breaches of any rules of the online community; • remove content that breaks the rules; • offer users a simple and easily accessible method of alerting the content producer to breaches of any rules of the online community; • remove content that breaks the rules; Before uploading age-sensitive editorially curated content onto a social networking site, be aware of the site's terms and conditions. Be sensitive to minimum age requirements on different social networking sites. The terms and conditions of each online space should also include clear reporting mechanisms for infringements of such rules.

Creating a safer and age-appropriate online environment	Companies offering curated digital content can help create a safer and more enjoyable digital environment for children and young people of all ages by taking the following actions:
	Work with others in the industry to develop content classification/age rating systems that are based on accepted national or international standards and consistent with approaches taken in equivalent media. Where possible, content classifications should be consistent across different media platforms, for example, a film trailer in a movie theatre and on a smartphone would show customers the same classifications.
	Develop child-friendly and age-appropriate products for children and young people that are safe by design and complemented by a solid age-verification system.
	To help parents and others decide whether content is age-appropriate for children and young people, build applications and services in all media to align with content rating systems. Adopt appropriate age-verification methods to prevent children and young people from accessing age-sensitive content, sites, products or interactive services. Provide advice and reminders about the nature and age-classification of the content they are using.
	A company that offers audiovisual and multimedia services might want to provide a personal identification number to users who seek to access content that can be harmful for children and young people.
	Ensure pricing transparency for products and services, and information collected about users. Ensure that data collection policies comply with relevant laws concerning children and young people's privacy, including whether parental consent is required before commercial enterprises can collect personal information from or about a child.
	Ensure that advertising or commercial communication is clearly recognizable as such. Supervise content made available online and adapt it to the user groups who are likely to access it by, for example, establishing appropriate policies for online advertising to children and young people. If the content offering supports an interactive element, such as commenting, online forums, social networks, gaming platforms, chat rooms or message boards, communicate a clear set of "house rules" in customer-friendly language within the terms of service and user guidelines.
	Decide what level of engagement is desired before launching an online service. Services aimed at appealing to children should only present content that is suitable for a young audience. If in doubt, the national authorities in charge of child protection may be consulted.
	Provide clear and factual content labelling. Be mindful that users can arrive at inappropriate content by following links on third-party sites that bypass contextualizing pages.

Educating children, parents and educators about children's safety and their responsible use of ICTs	Companies offering curated digital content can complement technical measures with educational activities that are empowering for children by taking the following actions:
	Provide customers with specific and clear information about content, such as the type of content, age ratings/restrictions, strong language or violence and the corresponding parental controls available; and about how to report misuse and inappropriate or illegal content, and how reports will be handled. In the interactive world, this information should be provided in the form of content labels for each program.
	Encourage adults, especially parents, carers and educators, to be involved in children and young people's online content consumption, so that they can assist and guide children and young people in choosing content when making a purchase, and help establish rules of behaviour. Help children (and parents and carers) to learn to manage their screen-time and understand how to use technology in a way that feels good to them, including when to stop and do something else.
	Provide rules of use in clear and accessible language that encourage children and young people to be vigilant and responsible when they are navigating the Internet.
	Build age-appropriate tools, such as tutorials and help centres. Work with online or in-person prevention programmes and counselling clinics when appropriate. For example, if there is a risk of children and young people becoming too engaged with technology, making it difficult for them to develop personal relationships or take part in healthy physical activities, a site could provide a contact link for a helpline or counselling service. Make safety information, such as links to advice, prominent, easily accessible and clear when online content is likely to appeal to a high proportion of children and young people.
	Offer a parental guidance tool, such as a "lock" for control of content that can be accessed through a particular browser
	Cooperate with parents to ensure that information disclosed on the Internet about children does not put them at risk. How children are identified in editorially curated content requires careful consideration and will vary according to the context. Obtain children's informed consent when featuring them in programmes, films, videos etc., wherever possible, and respect any refusal to take part.

Promoting digital technology as a mode to further civic engagement	Companies offering curated digital content can encourage and empower children and young people by supporting their right to participation through the following actions:
	Develop and/or offer a range of high-quality, challenging, educational, enjoyable and interesting content that is age-appropriate and helps children and young people make sense of the world in which they live. In addition to being attractive and usable, reliable and safe, such content can contribute to children and young people's physical, mental and social development by providing new opportunities to entertain and educate. Content that empowers children to embrace diversity and be positive role models should be strongly encouraged.

5.3 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, 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 (Facebook Messenger, Groupme**,** Line, Tinder, Telegram, Viber, WhatsApp).
- 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 (Instagram, Facebook, SnapChat, TikTok).
- Primarily live streaming apps (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Service providers request a minimum age to sign up to the platforms but this is difficult to enforce as age-verification is reliant on reported age. Most services that connect new users with each other also allow location-sharing features, which make children and young people using these services even more susceptible to offline danger.

Table 4, which has been adapted from the rules applied by one of the largest social networks, provides guidance for providers of services hosting user-generated content and connecting new users on policies and actions they can take to enhance child online protection and children's participation.

Table 4: COP checklist for Feature C: Host user-generated content and connect users

Integrating child rights considerations into all appropriate corporate policies and management processes	Services hosting user-generated content and connecting users 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.
	Refer to the general guidelines in Table 1.
Developing standard processes to handle CSAM	In collaboration with government, law enforcement, civil society and hotline organizations, companies hosting user-generated content and connecting users can play a key role in combating CSAM by taking the following actions:
	Establish procedures for all sites to provide immediate assistance to law enforcement during emergencies and for routine inquiries.
	Specify that the business will cooperate fully with law enforcement investigations in the event that illegal content is reported or discovered and note details regarding such penalties as fines or cancellation of billing privileges.
	Work with internal functions such as customer care, fraud prevention and security to ensure that the business can submit reports of suspected illegal content directly to law enforcement and hotlines. Ideally, this should be done in a way that does not expose front-line staff to the content or revictimize the affected child/children and young people. To address situations where staff may be exposed to abusive material, implement a policy or programme to support staff resiliency, safety and well-being.
	Use terms of service and conditions to prohibit illegal content and behaviour, highlighting that: • harmful content, including suspected grooming of children with the intention of either contact or non-contact abuse, will not be tolerated; • illegal content, including the uploading or further dissemination of CSAM, will not be tolerated; • the company will refer to and collaborate fully with law enforcement investigations in the event that illegal content, or any breach of the child protection policy, is reported or discovered.
	Document the company's practices for handling CSAM, beginning with monitoring and extending to the final transfer and destruction of the content. Include a list of all personnel responsible for handling the material in the documentation.
	Adopt policies regarding ownership of user-generated content, including the option to remove user-created content at the user's request. Remove content that violates the provider's policies and alert the user who has posted it about the violation.

Developing standard processes to handle CSAM (*cont.*)	Indicate that a user's failure to comply with policies for acceptable use will have consequences, including: • removal of content, suspension or closure of their account; • revoking their ability to share particular types of content or use certain features; • preventing them from contacting children; • referring issues to law enforcement.
Developing standard processes to handle child sexual abuse material	Promote reporting mechanisms for CSAM or any other illegal content and ensure that customers know how to file a report if they discover such content. Build systems and provide trained staff to assess issues on a case-by-case basis and take appropriate action. Establish comprehensive and well-resourced user-support operation teams. Ideally, these teams would be trained to handle different types of incidents in order to ensure that an adequate response is provided and appropriate actions are taken. When the user files a complaint, depending on the type of incident, it should be routed to appropriate staff. The company might also set up special teams to handle user appeals for instances when reports may have been filed in error.
	Have processes in place to immediately remove or block access to CSAM, including notice and takedown processes to remove illegal content as soon as it is identified. Ensure that third parties with whom the company has a contractual relationship have similarly robust notice and takedown processes in place. If legislation allows, the material can be kept for evidence of a crime in case of investigations.
	Develop technical systems that can detect known illegal content and can prevent it from being uploaded, including to private groups, or flag it for immediate review by the company's safety team. Take all relevant measures to safeguard services from being misused to host, disseminate or create CSAM. Where possible, create proactive technical measures to analyse the objects and metadata linked to a profile to detect criminal behaviour or patterns, and take appropriate action.
	If the application or service allows customers to upload and store photographs on servers that are owned or operated by the company, have processes and tools in place to identify images that are most likely to contain CSAM. Consider proactive identification techniques such as scanning technology or human review.

Creating a safer and age-appropriate online environment	Service providers offering user-generated content and connecting users can help create a safer, more enjoyable digital environment for children of all ages by taking the following actions:
	Communicate in customer-friendly language within the terms of service and user guidelines a clear set of "house rules" that define: • the nature of the service and what is expected of its users; • what is and is not acceptable in terms of content, behaviour and language as well as prohibiting illegal usage; • the consequences of any breach, for example, reporting to law enforcement and suspension of the user's account.
	Key safety and legal messages should be presented in an age-appropriate format (i.e. utilizing intuitive icons and symbols) both at signup and in a timely manner as different actions are taken on the site.
	Make it easy for customers to report concerns about misuse to customer care, with standard and accessible processes in place to deal with different concerns, such as receiving unwanted communications (spam, bullying) or seeing inappropriate content.
	Provide age-appropriate content-sharing and visibility settings. For example, make privacy and visibility settings for children and young people more restrictive than the settings for adults by default.
	Enforce minimum age requirements and support the research and development of new age-verification systems such as biometrics, using known international standards for the development of such tools. Take steps to identify and remove underage users who have misrepresented their age to gain access. Consideration needs to be given to the additional personal data collection that this may entail and the need to limit the collection and storage of this information and its processing. If not already in place, set up appropriate sign-on processes to determine whether users are old enough to access the content or service without compromising their identity, location and personal details. Use nationally established functional age-verification systems as appropriate, where relevant measures for data privacy of the child subjects exists. A reporting function or a help desk/centre that can encourage users to report people who have falsified their ages.

Creating a safer and age-appropriate online environment (*cont.*)	Protect younger users from uninvited communication and ensure that privacy and information-collection guidelines are in place.
	Find ways to review hosted images and videos and delete inappropriate ones when detected. Tools such as hash scanning of known images and image recognition software are available to assist with this. In services targeted at children, photos and videos can be checked beforehand to make sure that children do not publish sensitive personal information about themselves or others.
	A number of measures may be used to control access to user-generated content and protect children and young people online against inappropriate or illegal content. Make sure that secure passwords are used as a step towards protecting children and young people in gaming and other social media settings. Other techniques include: • reviewing discussion groups to identify harmful subject matter, hate speech and illegal behaviour, and deleting such content when it is found to violate the terms of use; • developing tools to actively seek and remove content that is illegal or in breach of the company's terms of condition and service, as well as tools to prevent uploading of known illegal content to the site; • pre-moderating message boards with a team of specialized children and young people's moderators who screen for content that is in contradiction to the published "house rules". Each message can be checked before it is published, and moderators can also spot and flag suspicious users, as well as users in distress; • establishing a team of community hosts who serve as the first point of contact for the moderators when they have concerns about a user.
	Be responsible for reviewing commercial content, including in forums, social networks and gaming sites. Implement appropriate standards and rules to protect children from age-inappropriate advertising and establish clear limits for online advertising to children and young people.

Educating children, parents and educators about children's safety and their responsible use of ICTs	Service providers offering user-generated content can complement technical measures with educational and empowerment activities by taking the following actions:
	Create a section dedicated to safety tips, articles, features and dialogue about digital citizenship, as well as links to useful content from third-party experts. Safety advice should be easily spotted and provided in easy-to-understand language. Platform providers are also encouraged to have a uniform navigation interface across different devices, such as computers, tablets or mobile phones.
	Offer parents clear information about the types of content and services available, including, for example, an explanation of social networking sites and location-based services, how the Internet is accessed via mobile devices, and the options available for parents to apply controls.
	Inform parents about how to report abuse, misuse and inappropriate or illegal content, and how the report will be handled. Let them know what services are age-restricted and other ways to behave safely and responsibly when using interactive services.
	Establish a "trust and reputation"-based system to encourage good behaviour and enable peers to teach best practices to each other by example. Promote the importance of social reporting, which allows people to reach out to other users or trusted friends to help resolve a conflict or open a conversation about troubling content.
	Provide advice and reminders about the nature of a given service or content and how to enjoy it safely. Build community guidelines into interactive services, for example, with safety popups that remind users of appropriate and safe behaviour, such as not giving out their contact details.
	Cooperate with parents and guide them to ensure that information disclosed on the Internet about children does not put them at risk. Obtain children's informed consent when featuring them through their own user-created content, wherever possible, and respect any refusal.
Promote digital technology as a mode to further civic engagement	Services hosting user-generated content can encourage and empower children and young people by supporting their right to participation.
	Refer to the general guidelines in Table 1.

5.4 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.

"Because of the exponential advancement of artificial intelligence-based technologies over the past few years, the current international framework that protects children's rights does not explicitly address many of the issues raised by the development and use of artificial intelligence. However, it does identify several rights that may be implicated by these technologies, and thus provides an important starting place for any analysis of how children's rights may be positively or negatively affected by new technologies, such as rights to privacy, to education, to play, and to non-discrimination."[18]

The application of AI can affect the impact on children of different services that are used on social networks, such as video streaming platforms. Machine-learning algorithms, the recommendation engine primarily employed by popular video-sharing platforms, are optimized to ensure maximum views of specific videos within a given time.[19] Touchscreen technology and the design of these platforms allow very young children to browse and navigate this content. There is a particular concern that algorithms that use recommended videos can trap children in "filter bubbles" of poor or inappropriate content. As children are particularly susceptible to content recommendations, shocking "related videos" can grab their attention and divert them away from more child-friendly programming.[20]

AI also has an impact on child online protection with regard to smart toys. The distinct processes involved in the operation of smart toys come with their own challenges, i.e. the toy (which interfaces with the child), the mobile application, acting as access point for Wi-Fi connection, and the toy's/consumer's personalized online account, where data is stored. Such toys communicate with cloud-based servers that store and process data provided by the children who interact with the toy. This model has privacy concerns if security is not applied at every layer, which has been demonstrated by the many cases of hacking in which personal details were leaked. Moreover, some of the hacked devices (including smart web-enabled devices such as baby monitors, voice assistants etc.) can be used for surveillance of users without their knowledge or consent.

When integrating response mechanisms to detected threats against children using these devices by, for example, providing tips and recommendations based on detected behaviour (as mentioned earlier with the BBC Own It app), it is crucial that the companies designing the smart devices base these recommendations on evidence and develop them in consultation with child protection and child safeguarding experts.

While some companies are advancing principles for the ethical use of AI,[21] it is not clear if there are any public policies aimed at AI and children.[22] Several technology and trade associations, and computer science groups, have drafted ethical principles with regards to AI.[23] However, these do not explicitly refer to child rights, ways in which these AI technologies may create risks for children, or proactive plans for mitigating those.

---

18 UNICEF and UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.
19 Ibid.
20 Ibid.
21 See Microsoft, "Salient Human Rights Issues", Report - FY17; and Google, "Responsible Development of AI" (2018).
22 Microsoft Official Blog, "The Future Computed: Artificial Intelligence and its role in society", 2018.
23 The Guardian, "'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft", 2016.

"Like corporations, governments around the world have adopted strategies for becoming leaders in the development and use of AI, fostering environments congenial to innovators and corporations."[24] It is unclear, however, how such national strategies directly address children's rights.

Improving Facebook's handling of suicide and self-injury related content

In 2019, Facebook began hosting regular consultations with experts from around the world to discuss some of the more difficult topics associated with suicide and self-injury. These include how to deal with suicide notes, the risks related to depressing content online and newsworthy depictions of suicide. Further details of these meetings are available on Facebook's new Suicide Prevention page, in its Safety Center. These consultations resulted in several improvements to the way Facebook handles this type of content. Policy regarding self-harm, for example, was strengthened to prohibit graphic cutting images to avoid unintentionally promoting or triggering self-harm. Even when someone is seeking support or expressing themselves to aid their recovery, Facebook now displays a sensitivity screen over images of healed self-harm cuts. This type of content is now being discovered through the application of AI whereby action on potentially harmful content, including removing it or adding sensitivity screens, can be taken automatically. From April to June 2019, Facebook acted on more than 1.5 million pieces of suicide and self-injury content on its site and identified more than 95 per cent of it before it was reported by a user. During that same time period, Instagram acted on more than 800 thousand pieces of similar content, of which more than 77 per cent was detected before being reported by a user.

Identifying potential bullying or peer-to-peer violence in real time and messaging users

Instagram is putting in place AI to root out behaviour such as insults, shaming and disrespect. By using sophisticated reporting tools, moderators can quickly close the account owned by the perpetrator of online bullying.

[24] Ibid.

Good practice: Use of artificial intelligence in the identification of child sexual abuse material

Building on Microsoft's generous contribution of PhotoDNA to fight child exploitation and the recent launch of Google Content Safety API, Facebook has also developed technologies to detect child sexual abuse content.

Known as PDQ and TMK+PDQF, these technologies are part of a suite of tools Facebook uses to detect harmful content. Other algorithms and tools available to industry include pHash, aHash and dHash. The Facebook photo-matching algorithm, PDQ, owes much inspiration to pHash, although it was built from the ground up as a distinct algorithm with independent software implementation. The video-matching technology, TMK+PDQF, was developed jointly by Facebook's AI Research team and academics from the University of Modena and Reggio Emilia in Italy.

These technologies create an efficient way to store files as short digital hashes that can determine whether two files are the same or similar, even without the original image or video. Hashes can also be more easily shared with other companies and non-profit organizations.

PDQ and TMK+PDQF were designed to operate at high scale, supporting video-frame-hashing and real-time applications.

Some of the recommendations for businesses to align their principles when designing and implementing AI-based solutions targeting children are provided in Table 5.

The recommendations are based on UNICEF's work to develop global policy guidance on AI and children, which will be aimed at governments and industry. Please see https://www.unicef.org/globalinsight/featured-projects/ai-children for more information on the project. The recommendations also draw on UNICEF and UC Berkeley's paper on AI and Child Rights.[25]

[25] UNICEF and UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.

Table 5: COP checklist for Feature D: AI-driven systems

Integrating child rights considerations into all appropriate corporate policies and management processes	Providers of AI-driven systems 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.
	AI systems should be designed, developed, implemented and researched to respect, promote and fulfil child rights, as enshrined in the Convention on the Rights of the Child. Childhood, which is increasingly experienced in the digital environment, is a time dedicated to special care and assistance. AI systems should be leveraged to provide this support to its fullest potential.
	Incorporate an inclusive design approach when developing child-facing products, which maximizes gender, geographic and cultural diversity, and includes a broad range of stakeholders, such as parents, teachers, child psychologists, and, where appropriate, children themselves.
	Governance frameworks, including ethical guidelines, laws, standards and regulatory bodies, should be established to oversee processes which ensure that the application of AI systems does not infringe upon child rights.
Developing standard processes to handle CSAM	In collaboration with government, law enforcement, civil society and hotline organizations, providers of AI-driven systems play a key role in combating CSAM by taking the following actions:
	Refer to the general guidelines in Table 1.

Creating a safer and age-appropriate online environment	Providers of AI-driven systems can help create a safer and more enjoyable digital environment for children of all ages by taking the following actions:
	Adopt a multi-disciplinary approach when developing technologies that affect children and consult with civil society, including academia, to identify the potential impacts of these technologies on the rights of a diverse range of potential end-users.
	Implement safety by design and privacy by design for products and services addressed to or commonly used by children.
	As AI systems are data-hungry, companies using AI for their services should apply special vigilance with regard to the collection, processing, storage, sale and publishing of children's personal data. AI systems should be transparent, in that it should be possible to discover how and why a system made a particular decision or, in the case of a robot, acted the way it did. This transparency is crucial to developing trust and facilitating auditing, investigations and recourse when harm to children is suspected. Ensure that there are functional and legal mechanisms for recourse if children are, or claim to be, harmed through AI systems. Processes should be established for the timely redress of any discriminatory outputs, and oversight bodies set up for appeals and continual monitoring of children's safety and protection. Accountability and mechanisms for redress go hand in hand.
	Develop plans for handling especially sensitive data, including revelations of abuse or other harm that may be shared with the company through its products. Digital platforms and AI systems should minimize the collection of data on children and maximize children's control over the data they do create. Terms of use should be understandable for children to empower their awareness and agency.
Educating children, parents and educators about children's safety and their responsible use of ICTs	Providers of AI-driven systems can complement technical measures with educational and empowerment activities.
	It should be possible to explain the purpose of AI systems to child users and their parents or carers to empower them to decide to use or refuse such platforms.

Promote digital technology as a mode to further civic engagement	Providers of AI-driven systems can encourage and empower children and young people by supporting their right to participation.
	Refer to the general guidelines in Table 1.
Using technology advances to protect and educate children	AI-driven systems should be developed to support children's development and well-being as an outcome in all system design, development and implementation. The best available and widely accepted development and well-being metrics should be their reference point. Companies should invest in research and development of ethical AI- based tools to detect acts of online CSAE, and online harassment and bullying, in collaboration with key experts on children's rights and children themselves. Advances in AI technology should be applied to target age-appropriate messaging for children without compromising their identity, location and personal details.

References

Text of the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)), and text as published in the Official Journal of the EU.

Revised AVMS (Audio Visual Media Services) amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities and Text as published in the Official Journal of the EU.

BBC policy:

- Child protection and safeguarding policy version 2017, revised 2018, and updated version 2019
- Working with young people and children at the BBC;
- Framework for Independent Production Companies working on BBC Productions on external providers rules about child protection;
- Guidance: Interacting with children and young people online on editorial guidelines for on-line activities.

Investigation proving non-respect of age verification for social media in the United Kingdom: 2016, 2017; 2020.

Glossary

The definitions below are mainly drawn from existing terminology set out in the Convention on the Rights of the Child, 1989, as well as by the Interagency Working Group on Sexual Exploitation of Children in the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, 2016 (Luxembourg Guidelines), by the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 2007, as well as by the UNICEF Global Kids Online report, 2019.

Adolescent

Adolescents are people aged 10–19 years. It is important to note that "adolescents" is not a binding term under international law, and persons below the age of 18 are considered to be children, whereas persons 18–19 years old are considered adults, unless majority is attained earlier under national law.[26]

Artificial intelligence

In the broadest sense, artificial intelligence (AI) refers indistinctly to systems that are pure science fiction (so-called "strong" AIs with a self-aware form) and systems that are already operational and capable of performing very complex tasks (systems described as "weak" or "moderate" AIs, such as face or voice recognition, and vehicle driving).[27]

Artificial-intelligence systems

An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.[28]

Alexa

Amazon Alexa, known simply as Alexa, is a virtual AI assistant developed by Amazon. It is capable of voice interaction, music playback, making to-do lists, setting alarms, streaming podcasts, playing audiobooks, and providing weather, traffic, sports, and other real-time information, such as news. Alexa can also control several smart devices using itself as a home automation system. Users are able to extend the Alexa capabilities by installing "skills" (additional functionality developed by third-party vendors, in other settings more commonly called apps such as weather programmes and audio features).[29]

[26] UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014.
[27] Council of Europe, "What's AI?".
[28] OECD, "Recommendation of the Council on Artificial Intelligence", 2019.
[29] UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014.

Best interest of the child

Refers to all the elements necessary to make a decision in a specific situation for a specific individual child or group of children.[30]

Child

In accordance with article 1 of the Convention on the Rights of the Child, a child is anyone below the age of 18, unless majority is attained earlier under national law.[31]

Child sexual exploitation and abuse

Describes all forms of sexual exploitation and sexual abuse, e.g. "(a) the inducement or coercion of a child to engage in any unlawful sexual activity; (b) the exploitative use of children in prostitution or other unlawful sexual practices; (c) the exploitative use of children in pornographic performances and materials",[32] as well as a "sexual contact that usually involves force upon a person without consent".[33] Child sexual exploitation and abuse (CSEA) increasingly takes place through the Internet, or with some connection to the online environment.

Child sexual exploitation and abuse material

The rapid evolution of ICTs has created new forms of online CSEA, which can take place virtually and do not have to include a physical face-to-face meeting with the child.[34] Although many jurisdictions still label images and videos of child sexual abuse "child pornography" or "indecent images of children", these Guidelines refer to the issues collectively as "child sexual abuse material" (CSAM). This term is in accordance with the Broadband Commission Guidelines and the WePROTECT Global Alliances' Model National Response[35] and more accurately describes the content. Pornography refers to a legitimate, commercialized industry, and as the Luxembourg Guidelines state, the use of the term:

"may (inadvertently or not) contribute to diminishing the gravity of, trivializing, or even legitimizing what is actually sexual abuse and/or sexual exploitation of children. The term 'child pornography' risks insinuating that the acts are carried out with the consent of the child and represent legitimate sexual material." When using the term CSAM, we refer to material that represents acts that are sexually abusive and/or exploitative to a child. This includes, but is not limited to, material recording the sexual abuse of children by adults, images of children included in sexually explicit conduct, and the sexual organs of children when the images are produced or used for primarily sexual purposes.

See the Luxembourg Guidelines for terms such as "computer or digitally generated child sexual abuse material".

30 See the United Nations Convention on the Rights of the Child.
31 UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014.
32 Article 34 of the United Nations Convention on the Rights of the Child.
33 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines), 2016.
34 The Luxembourg Guidelines (as above), 2016 and the UNICEF Global Kids Online report, 2019.
35 Broadband Commission for Sustainable Development, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online", 2019; WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response", 2016.

Children and young people

Describes all persons under the age of 18 years, whereby "children" (also referred to as "younger children" in these ITU guidelines) covers all persons under the age of 15 years and "young people" comprises persons in the 15–18 age group.

Connected toys

Connected toys connect to the Internet using technologies such as Wi-Fi and Bluetooth, and typically operate in conjunction with companion apps to enable interactive play for children. According to Juniper Research, in 2015 the market for connected toys reached USD 2.8 billion and is predicted to increase to USD 11 billion by 2020. These toys collect and store personal information from children including names, geolocation, addresses, photographs, audio and video recordings.[36]

Cyberbullying

Cyberbullying describes an intentionally aggressive act carried out repeatedly by either a group or an individual using digital technology and targeting a victim who cannot easily defend him or herself.[37] It usually involves "using digital technology and the Internet to post hurtful information about someone, purposely sharing private information, photos or videos in a hurtful way, sending threatening or insulting messages (via email, instant messaging, chat or texts), spreading rumours and false information about the victim or purposely excluding them from online communications".[38]

Cyberhate, discrimination and violent extremism

"Cyberhate, discrimination and violent extremism are a distinct form of cyber violence as they target a collective identity, rather than individuals, … often pertaining to race, sexual orientation, religion, nationality or immigration status, sex/gender and politics".[39]

Digital citizenship

Digital citizenship refers to the ability to engage positively, critically and competently in the digital environment, drawing on the skills of effective communication and creation, to practice forms of social participation that are respectful of human rights and dignity through the responsible use of technology.[40]

---

36 Jeremy Greenberg, "Dangerous Games: Connected Toys, COPPA, and Bad Security", Georgetown Law Technology Review, 2017.
37 Anna Costanza Baldry et al. "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities", Children and Youth Services Review, 2019.
38 The Luxembourg Guidelines, 2016 and the UNICEF Global Kids Online report, 2019 (as above).
39 UNICEF Global Kids Online report, 2019 (as above).
40 Council of Europe, "Digital Citizenship and Digital Citizenship Education".

Digital literacy

Digital literacy means having the skills a person needs to live, learn and work in a society where communication and access to information is increasingly through digital technologies like Internet platforms, social media and mobile devices.[41] It includes clear communication, technical skills and critical thinking.

Digital resilience

This term describes a child's capacity to cope emotionally with harm encountered online. It also refers to the emotional intelligence needed to understand when a child is at risk online, know how to seek help, learn from experience and recover when things go wrong.[42]

Governors

Describes all persons who hold a position in a school management or governance structure.

Grooming/online grooming

Grooming/online grooming, as defined in the Luxembourg Guidelines, refers to "the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate *either online or offline* sexual contact with that person". It is the criminal activity of becoming friends with a child…, in order to try to persuade the child to have a sexual relationship.

Information and communication technologies

Information and communication technologies (ICTs) describe all information technologies that emphasize the aspect of communication. This includes all Internet-connecting services and devices such as computers, laptops, tablets, smartphones, game consoles, and smartwatches.[43] It also includes services such as radio and television as well as broadband, network hardware and satellite systems.

Online gaming

Online gaming is defined as playing any type of single or multiplayer commercial digital game via any Internet-connected device, including dedicated consoles, desktop computers, laptops, tablets and mobile phones. The "online gaming ecosystem" is defined to include watching others play video games via e-sports, streaming or video-sharing platforms, which typically provide options for viewers to comment on or interact with the players and other members of the audience.[44]

---

41 Western Sydney University, "What is digital literacy?".
42 Dr. Andrew K. Przybylski, et al., "A Shared Responsibility: Building children's' online resilience", Virgin Media and Parent Zone, 2014.
43 UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014 (as above).
44 UNICEF, "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry", 2019.

Parental control tools

Software that allows users, typically a parent, to control some or all functions of a computer or other device that can connect to the Internet. Typically, such programmes can limit access to particular types or classes of websites or online services. Some also provide scope for time management, i.e. the device can be set to have access to the Internet only between certain hours. More advanced versions can record all texts sent or received from a device. The programmes normally will be password protected.[45]

Personal information

This term describes individually identifiable information concerning a person, which is collected online. This includes the full name, contact details, such as home and email addresses, and phone numbers, and fingerprints or facial recognition material, insurance numbers or any other factor that permits the physical or online contacting or localization of a person. In this context, it further refers to any information about a child and his or her entourage that is collected online by service providers online, including connected toys and the Internet of things, and any other connected technology.

Privacy

Privacy is often measured in terms of sharing personal information online, having a public social media profile, sharing information with people met online, using privacy settings, sharing passwords with friends, and concerns about privacy.[46]

Public service media

These are national broadcasters or media that have received their transmission licence based on a series of contractual obligations with the state or parliament. These obligations have been extended in many countries in recent years to tackle the consequences of the digital transformation through media and digital literacy programmes and obligations to address the digital divide.

Sexting

Sexting is commonly defined as the sending, receiving or exchanging of self-produced sexualized content including images, messages or videos through mobile phones and/or the Internet.[47] The creation, distribution and possession of sexual images of children is illegal in most countries. If self-produced sexual images of children are disclosed, adults should not view them. The sharing of sexual images by an adult with a child is always a criminal act, which can be harmful and it may be necessary to report such images and remove them.

---

45 UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014 (as above).
46 US Federal Trade Commission, "Children's Online Privacy Protection Act", 1998.
47 The Luxembourg Guidelines, 2016 (as above).

Sextortion or sexual extortion of children

Sextortion is the "blackmailing of a person with the help of self-generated images of that person in order to extort sexual favours, money, or other benefits from her or him under the threat of sharing the material beyond the consent of the depicted person (e.g. posting images on social media)".[48]

The Internet of Things

"The Internet of Things (IoT) represents the next step towards the digitization of our society and economy, where objects and people are interconnected through communication networks and report about their status and/or the surrounding environment."[49]

URL

This abbreviation stands for "uniform resource locator", the address of an Internet page.[50]

Virtual reality

"Virtual reality is the use of computer technology to create the effect of an interactive three-dimensional world in which the objects have a sense of spatial presence."[51]

Wi-Fi

Wi-Fi (Wireless Fidelity) is the group of technical standards that enable data transmission over wireless networks.[52]

48 The Luxembourg Guidelines, 2016 (as above).
49 European Commission, "Policy: The Internet of Things".
50 UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014 (as above).
51 NASA, "Virtual Reality: Definition and Requirements".
52 US Federal Trade Commission, "Children's Online Privacy Protection Act", 1998.

With the support of:

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

ISBN: 978-92-61-30411-9

Published in Switzerland
Geneva, 2020
Photo credits: Shutterstock