GUIDELINES FOR INDUSTRY ON CHILD ONLINE PROTECTION (LOCALIZED FOR BHUTAN)

VERSION 1.0
2023

GUIDELINES FOR INDUSTRY
ON
CHILD ONLINE PROTECTION
(LOCALIZED FOR BHUTAN)

VERSION 1.0

2023

Table of Content

ABSTRACT

In today's digital landscape, children and young people are active participants across various online platforms, necessitating comprehensive measures to safeguard their rights and well-being. This abstract summarizes key recommendations from the Child Online Protection (COP) checklist for Feature D, which centers on companies utilizing artificial intelligence (AI)-driven systems and their responsibilities in protecting children's rights and promoting their safe online experiences.

The integration of child rights considerations into corporate policies and management processes is paramount. AI systems must be designed with a commitment to upholding children's rights as outlined in the Convention on the Rights of the Child. This involves employing an inclusive design approach that takes into account diversity in gender, culture, and geography, with input from various stakeholders, including children themselves.

AI-driven system providers play a vital role in addressing issues such as child sexual abuse material (CSAM). Collaborative efforts with government entities, law enforcement agencies, civil society organizations, and hotline initiatives are crucial for combating CSAM. Standard procedures for promptly assisting law enforcement and cooperation with internal departments are essential aspects of this process.

Creating a safer online environment for children involves a multidisciplinary approach and proactive safety and privacy measures. Providers should exercise caution and responsibility in handling children's personal data, prioritize transparency, establish mechanisms for addressing grievances, and empower children with control over their data.

Educational initiatives are vital for ensuring that children, parents, and educators understand the functionality and objectives of AI systems, enabling informed decisions about platform usage. Additionally, promoting digital technology as a means to foster civic engagement aligns with children's rights to participate.

Advancements in AI technology present opportunities to protect and educate children effectively. Companies should allocate resources for ethical AI tools capable of identifying online threats and harassment, collaborating with children's rights experts, and leveraging AI to deliver age-appropriate content while safeguarding children's identity and personal information.

In a digital age where children's online experiences are increasingly vital, these guidelines provide a roadmap for AI-driven system providers to prioritize child online protection, uphold their rights, and contribute to the creation of a safer and more inclusive digital environment for all.

OVERVIEW

The purpose of this document is to guide stakeholders within the Information and Communication Technology (ICT) industry in the development of their resources about Child Online Protection (COP). These guidelines for child online protection within the industry are intended to establish a comprehensive, adaptable, and user-friendly framework. They serve the dual purpose of aligning with corporate visions and fulfilling the responsibility of safeguarding users, particularly children. Furthermore, these guidelines aim to lay the groundwork for fostering a safer and more secure utilization of Internet-based services and associated technologies for both present-day youth and future generations.

Functioning as a versatile toolkit, these guidelines also seek to enhance the success of businesses, regardless of their scale, by assisting various stakeholders in formulating and sustaining an appealing and sustainable business model. Simultaneously, they emphasize the comprehension of both legal and ethical obligations towards children and society at large.

As a response to the substantial advancements in technology and the convergence of various sectors, the Government Technology (GovTech) Agency, in collaboration with the International Telecommunication Union (ITU), the United Nations Children's Fund (UNICEF), and partners dedicated to COP, have adapted the ITU guidelines for a diverse array of companies engaged in the development, provisioning, or utilization of telecommunications or related activities in the provisioning of their products and services.

These industry guidelines for child online protection have been meticulously crafted through consultations with members of the COP Taskforce and have undergone extensive input from a broad spectrum of stakeholders, including civil society representatives, business leaders, academic experts, governmental bodies, media organizations, international entities, parents, educators, and young individuals.

The objectives of this document are as follows:

1. To establish a standardized reference point and offer guidance for the ICT and online industries, along with relevant stakeholders.
2. To offer direction to companies in the ICT sector regarding the identification, prevention, and mitigation of any adverse impacts that their products and services may have on the rights of children.
3. To provide guidance to companies in the ICT sector on how they can identify methods to promote the rights of children and encourage responsible digital citizenship among young individuals.
4. To propose fundamental principles that can serve as a foundation for national or regional commitments within all relevant industries. It is important to acknowledge that different types of businesses may employ diverse implementation models.

Scope

COP presents a multifaceted challenge encompassing various aspects, including governance, policy, operations, technology, and legal considerations. These guidelines aim to address, structure, and prioritize many of these dimensions by drawing from established models, frameworks, and recognized references.

The primary focus of these guidelines is to safeguard children across all aspects and potential risks within the digital realm. They emphasize best practices for industry stakeholders to consider when formulating, developing, and managing COP policies within their organizations. These guidelines not only offer direction on handling and mitigating illegal online activities, such as online Child Sexual Abuse Material (CSAM), which companies are obligated to combat through their services, but also extend their focus to other issues that may not universally be classified as crimes across all jurisdictions. These additional concerns encompass peer-to-peer violence, cyberbullying, online harassment, as well as matters related to privacy, general well-being, fraud, or other threats that might only pose harm to children under specific circumstances.

In pursuit of these objectives, these guidelines put forth recommendations for best practices in addressing the risks children encounter in the digital domain and offer guidance on how to create a secure online environment for them. They furnish insights into how the industry can collaborate to ensure the safety of children when using ICTs, the Internet, or any associated technologies or devices capable of connecting to these platforms. This encompasses a wide array of devices, such as mobile phones, gaming consoles, connected toys, wearable devices, the Internet of Things, and AI-driven systems. Consequently, these guidelines provide an overview of the central issues and challenges related to child online protection and propose actionable steps for businesses and stakeholders in developing local and internal COP policies. It is important to note that these guidelines do not encompass aspects related to the actual formulation or content of COP policies specific to individual industry practices.

Structure

Section 1 – Overview: This section serves to elucidate the purpose, scope, and intended audience of these guidelines.

Section 2 – Introduction to COP: Within this section, we present a comprehensive introduction to the matter of child online protection. It provides an overview, including essential background information, and takes into consideration the unique circumstances of children with disabilities. Additionally, this section references existing international and national models aimed at enhancing the online safety of children, which can serve as potential areas for industry stakeholders to intervene.

Section 3 – Key Areas of Safeguarding and Promoting Children's Rights: This section delineates five pivotal domains wherein companies can undertake actions to ensure the secure and positive utilization of ICTs by children.

Section 4 – General Guidelines: Within this section, we present recommendations tailored to all industry stakeholders concerning the safeguarding of children's well-being when utilizing ICTs and the promotion of responsible digital citizenship among children.

Section 5 – Feature-Related Checklists: This section focuses on specific recommendations for stakeholders, offering concrete guidance on respecting and supporting children's rights in the context of various features, including:

- Feature A: Provision of Connectivity, Data Storage, and Hosting Services
- Feature B: Provision of Curated Digital Content
- Feature C: Hosting User-Generated Content and Facilitating User Connections
- Feature D: AI-Driven Systems

Target audience

Building upon the United Nations Guiding Principles on Business and Human Rights[1],the Children's Rights and Business Principles emphasize the responsibility of businesses to uphold children's rights. This entails preventing any negative impacts associated with their operations, products, or services. These principles also distinguish between the concept of "respect," which signifies the minimum obligation of businesses to avoid harming children, and "support," which involves voluntary actions aimed at advancing the realization of children's rights. Businesses are obligated to ensure both the online protection of children and their access to information and freedom of expression, all the while promoting the constructive use of ICTs.

Traditional distinctions that have historically separated different segments of the telecommunications and mobile phone industries, as well as those between Internet companies and broadcasters, are rapidly eroding and becoming indistinct. The process of convergence is amalgamating these previously discrete digital streams into a unified current that reaches billions of people worldwide. The key to establishing a foundation for a safer and more secure utilization of the Internet and associated technologies lies in cooperation and collaboration. Governments, the private sector, policymakers, educators, civil society, parents, and caregivers all play pivotal roles in achieving this objective. Industry can take action in five crucial areas, as detailed in Section 3 of this document.

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

WHAT IS CHILD ONLINE PROTECTION?

Over the past decade, there have been significant transformations in the role and utilization of the Internet in people's lives. The widespread adoption of smartphones and tablets, the availability of Wi-Fi and 4G technology, and advancements in social media platforms and applications have led to an increasing number of individuals accessing the Internet for a variety of purposes.

In 2019, more than half of the global population was connected to the Internet. The majority of Internet users fall under the age of 44, with usage rates being particularly high among both 16 to 24-year-olds and 35 to 44-year-olds. On a global scale, one out of every three Internet users is a child (0 to 18 years old), and approximately 71 percent of young people are already online. In 2021, nearly 94.3 percent of households in Bhutan reported having Internet access, and in 2020, approximately 68 percent of students in Bhutan reported Internet usage[2]. The proliferation of Internet access points, mobile technology, and the growing variety of Internet-enabled devices, combined with the vast resources available online, present unprecedented opportunities for learning, sharing, and communication.

The advantages of ICT use encompass broader access to information regarding social services, educational resources, and healthcare guidance. As children, young people, and families turn to the Internet and mobile phones for information, assistance, and reporting instances of abuse, these technologies can play a crucial role in safeguarding children and young people from violence and exploitation. Child protection service providers also employ ICTs to collect and transmit data, thereby facilitating tasks such as birth registration, case management, family tracing, data collection, and the mapping of incidents of violence, among other functions.

Furthermore, the Internet has amplified access to information worldwide, allowing children and young people to explore a wide range of topics, access global media, pursue career prospects, and cultivate ideas for the future. ICT usage empowers children and young people to assert their rights, express their opinions, and enables them to connect and communicate with their families and friends. ICTs also serve as a primary medium for cultural exchange and a source of entertainment.

However, despite the profound benefits of the Internet, children and young people can also encounter several risks when using ICTs. They may be exposed to content unsuitable for their age or inappropriate contact, including from potential perpetrators of sexual abuse. Additionally, they can face reputational harm by sharing sensitive personal information online or through "sexting," often without fully comprehending the implications of their actions on themselves and others, including their long-term "digital footprints." Risks related to online privacy arise from data collection and the gathering and use of location information.

The Convention on the Rights of the Child, the most widely ratified international human rights treaty[3], outlines a comprehensive framework for the civil, political, economic, social, and cultural rights of children. It affirms that all children and young people are entitled to various rights, including the right to education, leisure, play, culture, appropriate information, freedom of thought, expression, and privacy. Moreover, it allows them to voice their opinions on matters that concern them, considering their evolving capacities. The Convention also places paramount importance on safeguarding children and young people from all forms of violence, exploitation, abuse, and discrimination, emphasizing the

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

[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.

child's best interests as the primary consideration in all matters affecting them. The responsibility for nurturing and supporting children and young people in their journey to adulthood rests with parents, caregivers, educators, community members, including community leaders and civil society participants. Governments play a crucial role in ensuring that all these stakeholders fulfill their responsibilities.

Regarding the protection of children's rights in the online realm, industries must collaborate to strike a delicate balance between the need to protect children and young people online and their right to access information and freedom of expression. Companies should prioritize targeted measures to protect them online without imposing excessive restrictions on children or other users. There is a growing consensus that promoting digital citizenship among children and young people and creating products and platforms that facilitate their positive use of Information and Communication Technologies (ICTs) should be a top priority for the private sector.

While online technologies offer numerous opportunities for children and young people to communicate, acquire new skills, express creativity, and contribute positively to society, they also introduce new risks to their safety. These risks include issues related to privacy, exposure to illegal content, harassment, cyberbullying, misuse of personal data, grooming for sexual purposes, and even child sexual abuse and exploitation. Additionally, children may face reputational harm, such as "revenge porn," stemming from the sharing of sensitive personal information online or through "sexting," which involves sending sexually explicit messages, photographs, or images between mobile phones. Online privacy concerns also arise when children use the Internet. Due to their age and evolving maturity, children often lack a full understanding of the risks associated with the online world and the potential negative consequences of their inappropriate behavior on both themselves and others.

Despite the advantages, the use of emerging and advanced technologies has downsides. Developments in Artificial Intelligence (AI), machine learning, virtual and augmented reality, big data, robotics, and the Internet of Things are poised to further transform children and young people's media practices. While these technologies are primarily designed to expand service delivery and enhance convenience, they may have unintended consequences and could be misused by child sex offenders. Creating a safe and secure online environment for children and youth necessitates the effective engagement of governments, the private sector, and all stakeholders. A key initial focus should be on enhancing the digital skills and literacy of parents and educators, an endeavor in which the industry can play a significant and sustainable role.

While some children may possess a good grasp of online risks and how to address them, this cannot be assumed for all children, particularly those belonging to vulnerable groups. The protection of children online holds immense significance under Target 16.2 of the United Nations Sustainable Development Goals, which strives to eradicate abuse, exploitation, trafficking, violence, and torture against children.

Since 2009, the COP Initiative, an international collaborative effort established by ITU, has been committed to raising awareness of online risks to children and the corresponding responses. The initiative brings together stakeholders from across the global community to ensure a safe and secure online environment for children worldwide. As part of this initiative, ITU published COP guidelines in 2009 for four distinct groups: children, parents, guardians, and educators; industry; and policymakers. Subsequently, Bhutan formed a taskforce, led by GovTech and supported by ITU and UNICEF, to adapt these guidelines to the specific context of Bhutan. The taskforce consists of justice and law enforcement agencies, regulators, organizations advocating for children's rights, social sectors, and industry representatives.

These guidelines define COP as an all-encompassing strategy designed to address all potential threats and harms that children and young people may encounter online or through online technologies. In this context, child online protection also encompasses harm to children that occurs offline but can be linked to evidence of online violence and abuse. Beyond examining children's online behavior and activities, child online protection considers the misuse of technology by individuals other than children themselves to exploit them.

All relevant stakeholders share the responsibility of helping children and young people leverage the opportunities offered by the Internet while simultaneously acquiring digital literacy and resilience to ensure their online well-being and protection. The safeguarding of children and young people is a collective responsibility, involving policymakers, industry, parents, caregivers, educators, and other stakeholders. To achieve this, they must ensure that children and young people can fully realize their potential both online and offline.

Child online protection, although lacking a universal definition, adopts a holistic approach to create secure, age-appropriate, inclusive, and participatory digital environments for children and young people. This approach is characterized by the following elements:

1. Effective responses, support, and self-help strategies in the face of online threats.
2. Prevention of potential harms.
3. Striking a dynamic balance between ensuring protection and providing opportunities for children to become responsible digital citizens.
4. Upholding the rights and responsibilities of both children and society.

Furthermore, due to the rapid advancements in technology and the borderless nature of the Internet, child online protection must be adaptable and agile to remain effective. New challenges will arise with the emergence of technological innovations, and these challenges will vary by region. Addressing these challenges necessitates global collaboration, as innovative solutions must be collectively developed to ensure the protection and well-being of children online.

BACKGROUND INFORMATION

As the Internet has become an integral part of the lives of children and young people, it is no longer feasible to separate the digital and physical realms. This interconnectedness has brought about significant empowerment. The online environment enables children and young people to overcome disadvantages and disabilities, offering new avenues for entertainment, education, engagement, and building relationships. Modern digital platforms serve as multifaceted spaces for a wide range of activities, often providing multimedia experiences.

Access to technology and the ability to use and navigate it are deemed essential for the development of young individuals. Children begin using ICTs at an early age, underscoring the importance of recognizing that they often start using platforms and services before they reach the minimum age defined by the tech industry's compliance requirements. Consequently, it is crucial for all stakeholders to understand that education should be seamlessly integrated into all online services utilized by children, alongside protective measures.

Children in the digital world

Internet access: In 2019, over half of the global population, accounting for 53.6 percent, was using the Internet, totalling an estimated 4.1 billion users. Remarkably, one out of every three Internet users is a child under the age of 18, according to UNICEF. Worldwide, 71 percent of young people are already connected online. Furthermore, in 2021, 94 percent of households in Bhutan reported having Internet access[4], and in 2020, about 68 percent of students in Bhutan confirmed their usage of the Internet[5].

In defiance of the minimum age requirements imposed by various online platforms, Ofcom, the United Kingdom's communications regulator, estimates that nearly 50 percent of children aged 10 to 12 years already possess social media accounts[6]. Moreover, eight out of every ten students are proficient in using social media platforms such as Facebook, Instagram, Snapchat, LINE, and WeChat to share ideas, engage in discussions, and collaborate with others, as reported by the DKAP. Consequently, children and young people have become a substantial, enduring presence on the Internet. The Internet serves not only as a means of social interaction but also as a tool for various social, economic, and political purposes, transforming into an integral family and consumer product or service that significantly influences the way families and young individuals lead their lives.

In 2017, at the regional level, access to the Internet for children and young people was closely associated with the level of national income. Typically, low-income countries exhibited lower levels of child Internet users in comparison to high-income countries. Most children and young people in various countries tend to spend more time online during weekends than on weekdays, with adolescents aged 15 to 17 spending the longest durations online, ranging from 2.5 to 5.3 hours, depending on the specific country. A focus group discussion (FGD) with students in Bhutan revealed that they spend approximately 5 to 6 hours on smartphones and the Internet.

Internet use: Among children and young people, the primary device for accessing the Internet is the mobile phone, followed by desktop computers and laptops. A 2020 survey in Bhutan estimated that 85 percent of students have access to smartphones at home, with laptops (41 percent) and tablets (23 percent) also being common. During weekdays, children and young people spend an average of two hours online each day, which increases to four hours per day on weekends. While some individuals feel constantly connected, there are still those who lack Internet access at home. In practice, most children and young people who use the Internet employ multiple devices, and those who connect at least weekly may utilize up to three different devices. Generally, older children and those in wealthier countries tend to use a greater number of devices, and in most surveyed countries, boys use slightly more devices than girls.

The most popular online activity among both girls and boys is watching or downloading music, videos, and photos. Globally, over three-quarters of Internet-using children and young people report watching videos online at least once a week, either alone or with family members. In Bhutan, around 74 percent of children reported enjoying watching or downloading photos and videos[7].

[4] Royal Government of Bhutan (Ministry of Information and Communication). 2021. "National ICT Household Survey, 2021".
[5] Royal Government of Bhutan (Ministry of Education). 2020. "Digital Kids Asia Pacific: The Country Report Bhutan".
[6] BBC, "Under-age social media use 'on the rise', says Ofcom".
[7] Royal Government of Bhutan (Ministry of Information and Communication). 2021. "National ICT Household Survey, 2021".

Many children and young people are considered "active socializers" and use various social media platforms such as Facebook, Twitter, TikTok, or Instagram. They also engage in online political discussions and express their opinions through blogging.

Participation in online gaming varies by country, typically aligning with the ease of Internet access for children and young people. However, the availability and affordability of online games are rapidly evolving, and the age at which children and young people begin accessing online games is decreasing. In Bhutan, eight out of ten children prefer downloading and playing online games, according to the ICT Survey.

On a weekly basis, between 10 and 30 percent of Internet-using children and young people, as surveyed in selected countries, engage in creative online activities. Additionally, many children and young people of all ages utilize the Internet for educational purposes, such as homework, catching up on missed classes, or seeking health information online. Older children tend to have a greater appetite for information compared to their younger counterparts.

Online child sexual exploitation and abuse: The incidence of online child sexual exploitation and abuse (CSEA) is increasing at an alarming rate. A decade ago, there were fewer than one million reported files of child abuse material. However, in 2019, this number had skyrocketed to 70 million, representing an almost 50 percent increase compared to 2018 figures. Furthermore, for the first time, videos of abuse have surpassed photos in reports to authorities, highlighting the urgent need for new tools to address this concerning trend. Victims of online CSEA span across all age groups but are becoming progressively younger. In 2018, the INHOPE network of hotlines observed a shift in victim profiles from pubescent to prepubescent. Additionally, research conducted by ECPAT International and INTERPOL in 2018 revealed that younger children were more likely to experience severe abuse, including torture, violent rape, or sadistic acts. Shockingly, this includes infants who are only days, weeks, or months old. Although girls are more frequently affected, abuse against boys may be more severe. The same report indicates that 80 percent of victims mentioned in reports were girls, 17 percent were boys, and children of both genders were mentioned in 3 percent of assessed reports[8].

Here are some key data points:[9]

- One in three Internet users worldwide is a child.
- Every half second, a child goes online for the first time.
- Approximately 800 million children use social media.
- At any given moment, an estimated 750,000 individuals online are seeking to connect with children for sexual purposes.
- There are over 46 million unique images or videos of child sexual abuse material (CSAM) in the EUROPOL repository.
- Over 89 percent of victims are aged between 3 and 13 years old.

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

The Impact of different platforms on children's digital experiences

The Internet and digital technology offer both advantages and risks to children and young people, and some of these are detailed below.

When children engage with social media, they have the opportunity to explore, learn, communicate, and develop essential skills. Social networks are viewed by children as platforms that enable them to discover their personal identity in a safe environment. It's crucial for young people to possess the relevant skills and know how to address privacy and reputation-related issues.

However, surveys indicate that most children are using social media before reaching the minimum age of 13, and age verification services are often weak or non-existent. Consequently, children face substantial risks. Additionally, while children express a desire to acquire digital skills, become responsible digital citizens, and manage privacy settings, they typically think about privacy concerning their friends and acquaintances – "What can my friends see?" – rather than considering the implications for strangers and third parties. This, combined with children's innate curiosity and a generally lower threshold for risk, can render them vulnerable to grooming, exploitation, bullying, or exposure to harmful content or contact.

The widespread popularity of image and video sharing through mobile apps, particularly the use of live streaming platforms by children, introduces additional privacy concerns and risks. Some children are creating and sharing sexual images of themselves, friends, and siblings online. In 2019, nearly a third (29 percent) of all webpages monitored by the Internet Watch Foundation (IWF) contained self-generated imagery. Of these, 76 percent depicted girls aged 11–13, with most images taken in their bedrooms or another room within a home setting. For some, especially older children, this behavior may be seen as a natural exploration of sexuality and sexual identity. However, for others, particularly younger children, there may be coercion by an adult or another child. Regardless of the circumstances, such content is illegal in many countries and may subject children to prosecution or further exploitation, grooming, or extortion.

Similarly, online gaming allows children to exercise their fundamental right to play, build networks, spend time with friends, make new acquaintances, and develop important skills. While these experiences can be overwhelmingly positive, in some instances, when left unmonitored and unsupported by a responsible adult, gaming platforms can pose risks to children. These risks encompass excessive play, financial hazards related to in-game purchases, the collection and monetization of children's personal data by industry entities, cyberbullying, hate speech, violence, exposure to inappropriate behavior or content, grooming, and the use of real, computer-generated, or virtual reality images and videos that depict and normalize child sexual exploitation and abuse (CSEA). These risks are not exclusive to the gaming environment but also apply to other digital environments where children spend their time.

Furthermore, advancements in technology have led to the emergence of the "Internet of Things" (IoT), where an increasing array of Internet-connected devices can communicate and network over the Internet. This category includes items such as toys, baby monitors, and AI-powered devices, which may introduce privacy risks and unwanted contact.

Good practice: Research: Microsoft conducted research on digital safety and cyberbullying in 2012, polling children aged 8–17 years from 25 countries. The results revealed several insights:

- On average, 54 percent of participants expressed concerns about being bullied online.
- 37 percent reported that they had experienced cyberbullying.
- 24 percent admitted to bullying someone online.
- The survey also found that fewer than three in 10 parents had discussed online bullying with their children. Since 2016, Microsoft has been conducting regular research on online risks, releasing annual Digital Civility Index reports. In Bhutan, around 14 percent of respondents reported being exposed to cyberbullying, with a higher proportion in urban areas[10].

FACES is a multimedia program produced by NHK Japan and a consortium of various public service broadcasters. It features stories of victims of both online and offline bullying from around the world. The program consists of portraits of adolescents who explain on camera how they responded to attacks on the Internet. The series, available in various languages, has been adopted by organizations such as Facebook, UNESCO, and the Council of Europe.

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

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

Good practice: Technology: The Google Virtual Reality Action Lab explores the potential of virtual reality in promoting youth engagement against offline and online bullying[11].

In September 2019, the BBC introduced the "Own IT" mobile application, targeting children aged 8–13 years who are receiving their first smartphones. This app aligns with the BBC's commitment to supporting young people in today's evolving media landscape and follows the successful launch of the Own IT website in 2018. The app employs advanced machine-learning technology to monitor children's smartphone activity and allows children to self-report their emotional well-being. It utilizes this data to provide tailored content and interventions aimed at helping children maintain a positive and healthy online experience. The app offers friendly and supportive reminders and guidance when a child's behavior deviates from the norm. Users can access the app when seeking assistance, and it also provides instant, on-screen advice and support through a specially designed keyboard. Key features include:

[10] Royal Government of Bhutan (Ministry of Information and Communication). 2021. "National ICT Household Survey, 2021".
[11] For more information see, Alexa Hasse et al., "Youth and Cyberbullying: Another Look", Berkman Klein Center for Internet & Society, 2019.

- Encouraging users to reconsider sharing personal information, such as mobile numbers, on social media.
- Assisting users in understanding how their messages may be perceived by others before sending them.
- Tracking mood changes over time and offering guidance on improving the situation if necessary.
- Providing information on topics like the impact of late-night phone use on well-being.

The app incorporates specially commissioned content from various BBC sources, offering valuable materials and resources to help young people make the most of their online experiences and develop healthy online behaviors. It facilitates constructive conversations between young people and parents about online experiences but does not provide reports or feedback to parents, and no user data is transmitted from the device. The app does not collect personal data or user-generated content, as all machine learning processes occur within the app and the user's device. Training of the machine learning models is conducted separately on training data to ensure privacy is maintained.

The special situation with disabilities

Children and adolescents with disabilities encounter online risks similar to their peers without disabilities. However, they may also confront specific risks linked to their disabilities. These individuals often experience exclusion, stigmatization, and various barriers—physical, economic, societal, and attitudinal—that hinder their participation in their communities. These challenges can negatively affect children with disabilities, driving them to seek social interactions and friendships in online spaces. While these online interactions can be positive, aiding in self-esteem building and support network creation, they can also expose these children to increased risks of grooming, online solicitation, and sexual harassment. Research indicates that children and young people facing offline difficulties and those with psychosocial challenges are at a higher risk of such incidents[12].

In essence, children who are victimized offline are more likely to face victimization online. This places children with disabilities at a heightened online risk, despite their greater need for online engagement. Studies reveal that children with disabilities are more prone to various forms of abuse,[13] particularly sexual victimization. Such victimization can encompass bullying, harassment, exclusion, and discrimination rooted in a child's actual or perceived disability, as well as aspects related to their disability, such as behavior, speech, or the use of equipment or services[14].

Perpetrators of grooming, online solicitation, and sexual harassment targeting children and young people with disabilities can include not only preferential offenders who target minors but also those who specifically target individuals with disabilities. This category may encompass "devotees"—non-disabled individuals with a sexual attraction to persons with disabilities, often pretending to have disabilities themselves[15]. Their actions may involve downloading and sharing photos and videos of children and young people with disabilities, which, while innocuous in nature, are often disseminated through dedicated forums or social media accounts. Reporting tools on such platforms often lack appropriate mechanisms to address these actions.

[12] Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content", Berkman Center for Internet & Society, 2008.
[13] UNICEF, "State of the World's Children Report: Children with Disabilities," 2013.
[14] 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.
[15] Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder", Sexuality and Disability, 1997.

Additionally, concerns exist regarding "sharenting," where parents share information and photos of their children and adolescents online. This practice can violate a child's privacy, potentially lead to bullying and embarrassment, and have adverse consequences in the future[16]. Some parents of children with disabilities may share information or media of their child in search of support or advice, inadvertently putting their child at risk of privacy breaches both now and in the future. These parents also face the risk of being targeted by individuals offering treatments, therapies, or so-called "cures" for their child's disability, who may not always have their best interests at heart. Similarly, some parents of children and young people with disabilities may become overprotective due to their lack of knowledge on how to guide their child's Internet use or protect them from bullying or harassment[17].

Furthermore, some children and young people with disabilities may encounter difficulties accessing online environments due to design inaccessibility (e.g., apps that do not allow text size adjustments), denial of requested accommodations (e.g., screen reader software or adaptive computer controls), or the need for appropriate support (e.g., coaching on equipment usage or one-on-one assistance in navigating social interactions)[18].

EXISTING NATIONAL AND TRANSNATIONAL MODELS FOR CHILD ONLINE PROTECTION

Globally, various models are being adopted to ensure the safety of children and young people online. Industry stakeholders should view these models as valuable guidance for international initiatives and as a structured framework to guarantee their utmost efforts in protecting children and young people in the online space. The Internet industry comprises a diverse and intricate landscape, consisting of companies of varying sizes and functions. It is crucial that child protection is addressed not only by platforms and services centered on content but also by those supporting the foundational infrastructure of the Internet.

It's important to acknowledge that the ability of an industry to implement a comprehensive child protection policy is constrained by the resources it has available. Therefore, these guidelines recommend that industries collaborate to implement services aimed at safeguarding users. Through resource sharing and the pooling of engineering expertise, industries can more effectively establish "safe spaces" to prevent abuse.

Industry Cooperation:

An exemplary case of successful cooperation among industry stakeholders in the fight against online child sexual exploitation and abuse is the Technology Coalition.

Transnational Models:

Industries should incorporate relevant international guidelines into their organizational frameworks and adhere to any applicable national or transnational laws in the countries where they operate. They should not only consider legal measures but also assess the actions they can take and, whenever possible, implement global initiatives. Some of the models that offer principles for such initiatives include:

[16] UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy", Innocenti Discussion Paper 2017-03 .
[17] UNICEF, "Is there a ladder of children's online participation?", Innocenti Research Brief, 2019.
[18] 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.

- Five Country Ministerial Voluntary principles to counter online child sexual exploitation and abuse (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).
- The South Asia Initiative to End Violence Against Children.
- OECD Recommendation on Protection of Children Online (2012).

There are various national and international models that define the roles and responsibilities of the technology industry in addressing child online protection. While some of these models may not specifically target children, they apply to them as Internet users and provide general guidelines to the industry on regulatory policies, standards, and collaboration with other sectors. This document highlights the key principles of such models as they pertain to the ICT industry:

The Age Appropriate Design Code, the United Kingdom:

In early 2019, the Information Commissioner's Office introduced a proposed age-appropriate design code aimed at safeguarding children's data. The code is built on the best interests of the child, as outlined in the United Nations Convention on the Rights of the Child, and outlines several expectations for the industry. It consists of fifteen standards, including default-off location services for children, minimal data collection and retention of personal data, privacy-centered product design, and age-appropriate and accessible explanations.

The Harmful Digital Communications Act, New Zealand:

The 2015 Act criminalizes cyber abuse and addresses a wide range of harms, from cyberbullying to revenge pornography. Its objective is to discourage, prevent, and mitigate harmful digital communications. It makes posting digital communications with the intent to cause severe emotional distress to someone else illegal and establishes ten communication principles. The Act empowers users to report violations of these principles to an independent organization or seek court orders against the author or host of the communication if the issue is not resolved.

The eSafety Commissioner, Australia:

Established in 2015, the Australian eSafety Commissioner is the world's first government agency dedicated to combating online abuse and enhancing online safety for its citizens. The eSafety Commissioner combines various functions, including prevention through awareness campaigns, education, research, best practice guidance, early intervention, and harm mitigation through statutory regulatory schemes. These schemes enable the rapid removal of cyberbullying, image-based abuse,

and illegal online content. In 2018, the eSafety Commissioner launched Safety by Design (SbD), an initiative that prioritizes user safety and rights in the design, development, and deployment of online products and services. It outlines safety by design principles that encourage industry to take measures to better protect users online. These principles emphasize:

Service provider responsibilities: Safety should not solely rely on end-users, and preventive measures should be incorporated into service design to address known and anticipated harms.

User empowerment and autonomy: User dignity and best interests should be central, supporting user control and regulation of their experiences.

Transparency and accountability: These are fundamental for safety, ensuring services adhere to safety objectives and educating the public about addressing safety concerns.

The WePROTECT Global Alliance:

The WePROTECT Global Alliance places a central emphasis on assisting countries in creating coordinated multi-stakeholder approaches to combat online child sexual exploitation. This strategy is guided by its Model National Response, which serves as a blueprint for national efforts. It offers a framework for countries to use in addressing online child sexual exploitation, including specific commitments from ICT companies. These commitments pertain to:

1. Establishing notice and takedown procedures.
2. Reporting instances of online child sexual exploitation and abuse (CSEA).
3. Developing technological solutions.
4. Investing in effective Child Online Protection (COP) prevention programs and response services.

The Global Partnership and Fund to End Violence against Children were initiated by the United Nations Secretary-General in 2016 with a singular objective: to galvanize and support actions aimed at ending all forms of violence against children by 2030. This effort involves collaboration among over 400 partners spanning various sectors. Their work primarily focuses on rescuing and assisting victims, implementing technology solutions to detect and prevent offending, supporting law enforcement, advocating for legislative and policy reforms, and generating data and evidence to understand the extent and nature of online child sexual exploitation while considering children's perspectives[19].

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

KEY AREAS OF PROTECTING AND PROMOTING CHILDREN'S RIGHTS

This section delineates five essential domains where companies can take proactive measures to ensure the safety of children and young individuals when utilizing ICTs. These actions are aimed at fostering a positive and secure environment for their engagement with ICTs.

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

To effectively integrate child rights considerations, companies must take proactive measures to identify, prevent, mitigate, and, when necessary, address potential and actual adverse impacts on children's rights. The United Nations Guiding Principles on Business and Human Rights establish that all businesses and industries have a responsibility to uphold human rights, including those of children.

Industries should give special attention to children and young people as a vulnerable group when it comes to data protection and freedom of expression. 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 online without unlawful interference. Similarly, United Nations Human Rights Council Resolution 32/13 recognizes that the same rights individuals have offline must also be protected online, acknowledging the global and open nature of the Internet as a force for development.

In Bhutan, the Information, Communications and Media Act of 2018 provides a legal framework to protect the general public and specifically children and young individuals from undesirable influences. The Act mandates that media facilities, service providers, and vendors take reasonable steps to prevent offensive communications from reaching children and to prevent children from engaging in business transactions. The Child Care and Protection Act of 2011 requires mass media to assist in promoting child rights and responsibilities and preventing offenses committed by children through positive publications. Child Protection and Well-Being Indicators recognize the risks and harm that children may encounter online, calling for the timely collection of disaggregated data to assess these risks.

However, it's widely believed that Bhutan's legal and regulatory framework for online protection is insufficient. Therefore, Bhutanese companies should exercise enhanced due diligence to ensure that their policies and practices align with international legal standards. As youth civic engagement increasingly occurs through online communications, companies have a heightened responsibility to uphold the rights of children and young people, even in cases where domestic laws have not yet caught up with international standards.

Companies should establish a functional grievance mechanism at the operational level, providing a platform for individuals who believe their rights may have been violated to voice their concerns. These mechanisms should be designed to be accessible to children, their families, and those advocating for their interests.

In accordance with Principle 31 of the UN Guiding Principles on Business and Human Rights, these mechanisms must possess specific qualities. They should be considered legitimate, easy to use, predictable, fair, transparent, compatible with human rights, conducive to ongoing learning, and centered on engagement and dialogue. In conjunction with internal procedures for addressing adverse impacts, grievance mechanisms should ensure that companies have structured frameworks in place

to guarantee that children and young people have appropriate avenues to seek redress when their rights are at risk.

When companies adopt a compliance-oriented strategy for ensuring ICT safety, their primary focus is on adhering to national laws, following international recommendations in the absence of national regulations or when they are insufficient, and preventing any negative effects on the rights of children and young people. Through voluntary initiatives that support children and young people's rights to access information, freedom of expression, participation, education, and culture, these companies actively contribute to the advancement of children and young people's development and well-being.

Good practice: Policy and age-appropriate design: The app developer Toca Boca creates digital toys with a child-centric approach. Their privacy policy is designed to transparently communicate what data the company collects and how it's used. Toca Boca, Inc is a member of the PRIVO Kids Privacy Assured COPPA Safe Harbor Certification Program.

LEGO® Life serves as a safe social media platform for children under 13, allowing them to share their LEGO creations, find inspiration, and interact in a secure environment. To create an account, children don't need to provide personal information; instead, it requires a parent or guardian's email address. This platform offers an opportunity for children and families to have positive discussions about online safety and privacy.

Public Service Broadcasters like ARD and ZDF in Germany cater to audiences starting from 14 years old through their customized content on the online channel funk.net. Meanwhile, the BBC has introduced CBeebies, tailored specifically for children under the age of 6, with website content designed to suit the needs of various age groups.

Developing standard processes to handle CSAM

In 2022, the Internet Watch Foundation (IWF) conducted investigations into 375,230 reports suspected to contain child sexual abuse imagery. Out of these reports, 255,580 were confirmed to contain images or videos depicting children subjected to sexual abuse. Notably, IWF identified 51,369 instances of Category A child sexual abuse material online, marking the highest number to date. It's important to note that a significant portion, approximately 78 percent, of the reported content was self-generated. Each URL could potentially contain a substantial number of such images and videos[20]. Among the images addressed by the IWF, 40 percent depicted children aged 10 or younger, and a concerning 1,001 webpages depicted children aged 0–2 years, with 81 percent of them containing the most severe forms of sexual abuse, including rape and sexual torture. These troubling statistics emphasize the critical need for collaborative efforts involving industry, governments, law enforcement, and civil society to combat child sexual abuse material (CSAM).

Numerous governments are addressing the issue of disseminating and distributing CSAM through legislative measures, pursuing and prosecuting offenders, increasing awareness, and providing support to children and young people affected by abuse or exploitation. However, like many other countries, Bhutan currently lacks adequate systems for dealing with this problem. It is crucial to establish mechanisms that enable the public to report abusive and exploitative content of this nature. Industry, law enforcement, governments, and civil society must collaborate to establish legal frameworks that align with international standards. These frameworks should criminalize all forms of online child sexual

[20] Internet Watch Foundation, "IWF 2023 Annual Report".

exploitation and protect child survivors of such abuse or exploitation. They should also ensure that reporting, investigative, and content removal processes operate as efficiently as possible.

In addition, the industry should offer links to national hotlines or other locally available reporting channels. In cases where local reporting options are absent, the industry should provide links to relevant international hotlines, such as the United States National Center for Missing and Exploited Children (NCMEC) or the International Association of Internet Hotlines (INHOPE), which can be used to file reports.

Responsible companies are taking various measures to prevent their platforms and services from being used to disseminate CSAM. These measures include incorporating explicit prohibitions of such content or conduct in their terms and conditions or codes of conduct, establishing robust notice and takedown processes, and collaborating with and supporting national hotlines.

Moreover, some companies are employing technical measures to prevent the misuse of their services or networks for sharing known CSAM. For instance, certain Internet service providers are blocking access to URLs confirmed by an appropriate authority as containing CSAM if the website is hosted in a country lacking the necessary processes for rapid takedown. Others are employing 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 integrate all relevant services into their operations to prevent the dissemination of child sexual abuse.

Recognizing the risk associated with CSAM, service providers in Bhutan have adopted and implemented comprehensive child safeguarding policies and guidelines that outline expected behaviors and responsibilities of staff members. These service providers are also investing in AI tools to identify CSAM. One telecommunications company shared its approach:

"Recognizing the importance of advanced technology, we are investing in AI-powered solutions to proactively detect and remove harmful content, including CSAM. Our well-defined protocols enable us to handle incidents of CSAM effectively, cooperating with law enforcement agencies to ensure a swift response and legal action. Furthermore, we understand the significance of utilizing AI tools to monitor children's online interactions, identify potential risks, and provide timely alerts for their protection and well-being."

Industry actors should commit to allocating proportional resources and continue developing and sharing technological solutions, preferably open source, to detect and remove CSAM.

Good practice: Technology: Microsoft employs a comprehensive strategy to promote responsible and secure technology use, addressing aspects such as the technology itself, self-regulation, partnerships, and educating and reaching out to consumers. Microsoft has integrated functionalities that empower individuals to better oversee their online safety. For example, they offer a feature called "Family Safety" that enables parents and caregivers to monitor their children's Internet activities.

Furthermore, Microsoft implements strict policies against harassment across its platforms. Users who violate these rules may face consequences such as account termination or, for severe violations, legal actions taken by law enforcement.

Microsoft has developed PhotoDNA, a tool that generates unique codes (hashes) for images and compares them to a database of known CSAM hashes. When it detects a match, it blocks the image.

PhotoDNA has been instrumental in removing millions of illegal photos from the Internet, aiding in the conviction of child sexual predators, and even helping law enforcement rescue potential victims before they suffer physical harm. However, it's important to note that PhotoDNA does not use facial recognition technology and cannot identify individuals or objects in the images.

PhotoDNA for Video, an extension of this tool, breaks down videos into key frames and creates hashes for those frames. This means that, just like PhotoDNA can detect manipulated images, PhotoDNA for Video can identify child sexual exploitation content that has been edited or inserted into videos that may seem harmless.

Furthermore, Microsoft has introduced Project Artemis, developed in partnership with organizations like The Meet Group, Roblox, Kik, and Thorn. This tool is designed to identify child predators who groom children for online abuse in chat rooms. It utilizes Microsoft's patented technology to alert chat room administrators when moderation is required, helping to detect and report individuals attempting to exploit children for sexual purposes.

The Internet Watch Foundation (IWF) offers various services to industry members to protect their users from encountering CSAM. These services include a regularly updated list of blocked URLs containing live CSAM, a hash list of known criminal content related to CSAM, a list of cryptic keywords associated with CSAM, and information on domain names known to host child sexual abuse content, facilitating the swift removal of such domains.

Creating a safer and age-appropriate online environment

Ensuring a safer and age-appropriate online environment is crucial, just as it is essential to prioritize safety in other aspects of life, even in well-regulated traffic in cities where accidents can still occur. Similarly, the digital realm is not without risks, particularly for children and young people, who play various roles in their online experiences. These risks can be categorized into four main areas[21]:

1. **Inappropriate Content:** Children and young people might unintentionally come across inappropriate or illegal content while browsing the Internet. This could happen through seemingly harmless links in messages, blogs, or while sharing files. Bhutan InfoComm and Media Authority (BICMA) has established rules and regulations to assess content.
2. **Inappropriate Conduct:** People of various age groups, including children and adults, may use the Internet for harassment or exploitation. Children may engage in hurtful comments, sharing embarrassing images, or violating copyrights.
3. **Inappropriate Contact:** Both adults and young individuals can misuse the Internet to target vulnerable children or young people. They may attempt to create a seemingly meaningful relationship while having manipulative intentions. This can involve convincing the child to engage in sexual or abusive acts online, often using webcams or other recording devices, or trying to arrange in-person meetings. This process is commonly referred to as "grooming."
4. **Commercial Risks:** This category encompasses data privacy concerns related to the collection and utilization of children's data and digital marketing practices.Addressing online safety is a collective endeavor, involving collaboration among industry players, governments, and civil society to establish safety principles and practices. Industry should offer a range of technical solutions and services for parents, children, and young people. They should prioritize user-

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

friendly, safe, and age-appropriate product design. Additionally, tools for age verification that respect children's privacy rights and limit access to age-inappropriate content or contacts should be provided."Safety by design"[22] frameworks, including privacy considerations, must be integrated into the innovation and product design process. Children's safety and responsible technology use should be a primary consideration, not an afterthought.

Certain programs allow parents to monitor their children's text and communication activities. However, it's vital to have open discussions with children about the use of such programs to avoid them feeling like they are being spied on, which could undermine trust within the family.

Acceptable-use policies are a way for companies to define encouraged behavior and unacceptable activities for both adults and children. They should also outline the consequences of policy violations. Clear and transparent reporting mechanisms should be accessible to users concerned about content or behavior. Timely follow-up on reports is crucial, including providing information about the report's status. Companies should communicate decisions regarding reports and offer a method for further follow-up if the user is unsatisfied with the response.

Good practice: Reporting: Facebook, in its efforts to combat online sexual harassment, has collaborated with the European Union to support Project deSHAME, a joint initiative involving Childnet, Save the Children, Kek Vonal, and UCLan. The primary goal of this project is to increase the reporting of online sexual harassment among minors and enhance cooperation among various sectors to prevent and address such behavior.

In line with the project's objective of encouraging users to report inappropriate or distressing content, Facebook's Community Standards serve as guidelines for what is permissible on their platform. These standards also define the types of users who are prohibited from posting. To further enhance safety, Facebook has introduced features like the "Do you know this person?" tool, an "other" inbox for receiving messages from unfamiliar individuals, and a notification that appears on the news feed when it detects potential contact between a minor and an unfamiliar adult.

Online content and service providers should accurately describe the type of content or services they offer and the intended age group for their audience. These descriptions should align with existing national and international standards, relevant regulations, and guidance on marketing and advertising to children provided by appropriate classification organizations. This process can become more challenging when dealing with interactive services that allow user-generated content, such as message boards, chat rooms, and social networking platforms. When companies specifically target children and young people or when their services are primarily designed for younger audiences, there is a higher expectation for content clarity, user-friendliness, and security.

Companies are strongly encouraged to adhere to the strictest privacy standards when it comes to collecting, processing, and storing data related to children and young people. This is because children and young individuals may not fully comprehend the broader social and personal implications of sharing their personal information online or consenting to its use for commercial purposes. Services aimed at or likely to attract a predominantly young audience must carefully consider the risks associated with access to, or the collection and utilization of, personal information, including location data. These risks should be adequately addressed, and users should be informed. Companies should use clear and straightforward language and communication styles in their promotional materials, service access,

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

and the collection and use of personal information to facilitate user understanding and enable them to manage their privacy effectively. Users should have a clear understanding of what they are agreeing to in accessible language.

Good practice: Innovation: In 2018-2019, the UNICEF East Asia and Pacific Regional Office organized a series of five multi-stakeholder roundtables. These gatherings aimed to facilitate the sharing of promising practices from various industries in addressing online child sexual exploitation and abuse (CSEA). Participants included prominent private sector companies like Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Mongolia), Mobifone+ (Vietnam), Globe Telecom (the Philippines), True (Thailand), GSMA, as well as civil society partners such as INHOPE, ECPAT International, and Child Helpline International.

As part of the same project, in February 2020, UNICEF launched a Think Tank initiative to accelerate industry leadership in the East Asia and Pacific region in preventing violence against children in the online realm. This Think Tank serves as an incubator for generating innovative ideas, drawing on the unique insights and perspectives of industry actors involved in product creation and marketing. Its goals include the development of impactful educational materials, identification of effective delivery platforms, and the creation of an evaluation framework to measure the impact of these educational materials and messages aimed at children.

The Think Tank comprises participants from various organizations, including Facebook, Telenor, academic experts, United Nations agencies such as ITU, UNESCO, and UNODC, as well as others like the Australia eSafety Commissioner, ECPAT International, ICMEC, INTERPOL, and the End Violence Global Fund. During the inaugural meeting, which coincided with the ASEAN Regional Conference on Child Online Protection, experts, including representatives from Microsoft, gathered to explore technology and research possibilities for better tracking changes in online behavior based on the adoption of online safety materials and messages.

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

Technical measures play a crucial role in safeguarding children and young people online, but they are just one aspect of the overall strategy. Parental control tools, awareness campaigns, and education are equally vital components that empower and educate children, parents, caregivers, and educators. In Bhutan, parental awareness of online risks is relatively low, with only about one-third (36.2%) of households aware of their children's exposure to harmful online behavior, and even fewer (15%) aware of exposure to pornography or cyberbullying. Thus, there is a pressing need for increased awareness among parents and the general public.

While companies have a responsibility to encourage responsible and safe Internet use among children and young people, this responsibility is shared with parents, schools, and the children themselves. Many companies are investing in educational programs to help users, parents, caregivers, and educators make informed decisions regarding online content and services. They are also assisting parents and caregivers in guiding children toward safer and more responsible online and mobile experiences. This includes providing clear information about age-sensitive content, content prices, subscription terms, and cancellation procedures.

Moreover, it's crucial to provide children and young people with direct information about safe ICT use and positive behavior online. Companies can contribute by creating content that promotes respectful, kind, and open-minded interactions and educates users on how to address negative experiences such as online bullying or grooming.

Parents often have less understanding of the Internet and mobile devices than their children. Industry, in collaboration with government and educators, can help enhance parents' capacity to support their children in building digital resilience and acting as responsible digital citizens. This doesn't mean transferring all responsibility to parents but recognizing that they play a critical role in determining what's appropriate for their children and should be well-informed about the associated risks.

Education on online safety and responsible ICT use should be integrated into school curricula and provided to parents through various media channels, considering that not all parents use Internet services. This collaboration can cover topics such as monitoring activities, addressing online bullying or grooming, managing privacy settings, and facilitating discussions about sensitive issues with children of different age groups.

As content and services become more diverse, users of all ages will benefit from guidance on service usage and safety. While children should be taught responsible Internet use, they also need room for exploration and learning through experience. Allowing them to take some risks online can contribute to their growth, as long as there is adequate support from parents and companies to help them learn from uncomfortable experiences.

Good practice: Education: NHK Japan conducts a suicide prevention initiative for young individuals via Twitter: In Japan, there is a concerning spike in teenage suicides, particularly during the period when students return to school after their summer break. This surge is often attributed to the challenging transition back to their regular routines. NHK Heart Net TV, a production team associated with NHK Japan, has developed a multimedia program called "#On the Night of August 31st." This initiative seamlessly integrates television broadcasts, live streaming, and social media to establish a supportive platform where teenagers can openly express their emotions and concerns without apprehension.

Good practice: Education: Project deSHAME, funded jointly by Facebook and the European Union, also facilitates the development of resources aimed at various age groups, with a specific emphasis on children aged 9–13 years. As part of this initiative, a toolkit named "Step Up, Speak Up!" has been created, offering a wide range of educational materials, training resources, awareness-building tools, and practical instruments for implementing multisector strategies to prevent and respond to online issues. The project plans to share these educational materials with other European countries and global partners to advocate for the digital rights of young people.

Google has launched a series of educational programs, resources, and tools designed to promote online safety for young individuals. Among these initiatives is the Be Internet Awesome campaign, which focuses on digital citizenship and was developed in collaboration with organizations like ConnectSafely, the Family Online Safety Institute, and the Internet Keep Safe Coalition. This campaign is tailored for youngsters aged 8–11 years and includes a web-based game called Interland, which educates youth about fundamental digital safety concepts. Additionally, Google provides resources for educators through its Digital Citizenship and Safety Curriculum, which encompasses lesson plans covering five key thematic areas, including cyberbullying. Furthermore, Google has created an online course on digital citizenship and safety for educators working with students of all age groups, offering

additional support for integrating these topics into the classroom. Google also runs various programs that directly involve young individuals in online safety and digital citizenship initiatives. The global Web Rangers program is one such effort, teaching young people about online safety and encouraging them to design their campaigns promoting positive and secure Internet usage. Additionally, Google has established country-specific programs for young people, such as Internet Citizens and Internet Legends in the United Kingdom.

The European Broadcasting Union organizes the Eurovision Youth News Exchange, bringing together 15 European television broadcasters to exchange programs, formats, and solutions in both online and offline domains. In recent times, their programs have increasingly focused on educating children about digital literacy and raising awareness about Internet-related risks. Notably, successful initiatives include social media advertisements and news programs tailored for children, which have been produced by Super and Ultranytt, part of NRK, the public broadcaster of Norway.

Good practice: Strategic partnership: Under the support of the End Violence Against Children Fund, Capital Humano Y Social Alternativo established a partnership with Telefónica, the largest provider of Internet, cable, and telephone services in Peru, serving over 14.4 million customers, including more than 8 million Movistar mobile users. This collaboration led to several initiatives:

- Telefónica developed a virtual course on child online protection with technical assistance from Capital Humano y Social Alternativo. This course is now accessible on Telefónica's website, and the company is monitoring the enrollment and completion rates. The Peruvian Ministry of Education also agreed to offer access to this course on its official website.
- Capital Humano y Social Alternativo created an Internet safety booklet, which Telefónica distributed through its network of over 300 mobile sales centers. The goal is to educate Telefónica customers about online safety and the risks associated with child sexual exploitation and abuse (CSEA).
- Telefónica, with technical support from Capital Humano y Social Alternativo, developed an interactive game focusing on online CSEA. Customers waiting at Telefónica's stores can engage with this game during their wait time.
- Building on the successful partnership with Telefónica, Capital Humano Y Social Alternativo extended its collaboration to Econocable, an Internet and cable service provider operating in remote and low-income areas of Peru.

Promoting digital technology as a mode for increasing civic engagement

Article 13 of the United Nations Convention on the Rights of the Child emphasizes a child's right to freedom of expression, including seeking, receiving, and sharing information through various media and forms of communication. To uphold this right, companies must ensure that their technological solutions, legal frameworks, and policies aimed at protecting children from online harm do not inadvertently restrict their freedom of expression or access to valuable information necessary for their well-being. It is crucial to strike a balance where age verification systems don't hinder specific age groups from accessing content relevant to their development.

Moreover, businesses and industries can actively promote the rights of children and young people by providing tools and mechanisms that facilitate their participation. They can highlight the Internet's potential to encourage positive engagement in civic life, drive social progress, and contribute to

community sustainability and resilience. This may involve participating in social and environmental initiatives, holding authorities accountable, and empowering children and young people to access information about their rights, personal matters like sexual health, and issues impacting their communities.

Companies can also invest in creating online experiences tailored to children, young people, and families, ensuring these platforms promote learning, innovation, and problem-solving. Safety considerations should be integrated into product design from the outset.

Furthermore, businesses can play a proactive role in bridging the digital divide. To participate effectively in the digital world, children and young people need digital literacy skills. Those lacking these skills face disadvantages in accessing services, information, and opportunities. Companies can support initiatives aimed at fostering digital skills among children and young people, ensuring they become confident and connected digital citizens[23]. Public service media in various countries have been involved in efforts to promote digital and media literacy and address the digital divide. For instance, the Italian Parliament has proposed priorities for the national broadcaster that include closing the digital divide and ensuring child protection both online and offline, setting an example for other nations to follow.

Good practice: Multiagency collaboration: Microsoft has recently become part of the global initiative called Power of ZERO, which is spearheaded by the organization No Bully. This campaign is focused on empowering young children, along with the adults responsible for their well-being, to use digital technology responsibly and develop essential qualities such as empathy, inclusivity, and effective communication, which are at the core of digital citizenship.

The initiative provides free educational resources to early educators and families, with a specific emphasis on children aged 8 and under. These resources are designed to help young children cultivate what Power of ZERO refers to as the "12 powers for good." These powers encompass various life skills that enable children to navigate both the online and offline worlds successfully. Some of these skills include resilience, respect, inclusivity, and creativity. The goal is to establish a solid foundation for children from a young age, promoting their positive development in both digital and real-life environments.

General guidelines for industry

Table 1 provides a set of overarching recommendations for the industry to identify, prevent, and address any potential negative impacts of their products and services on the rights of children and young people. It also offers guidance on how to encourage the positive and responsible use of ICTs by children and young people.

It's important to note that not all of the steps outlined in Table 1 will be applicable to every company or service, as the relevance may vary. Additionally, some services may require steps beyond what is mentioned in this table, and this table should be considered in conjunction with the more specific checklists provided in Tables 2–5. These feature-specific checklists offer additional guidance tailored to specific types of services and may overlap in certain areas, as they are designed to address the unique aspects of each service.

[23] For examples of youth participation from the mobile community.

Table 1: General guidelines for Industry

Sl. No.	Key Areas for consideration	Description
1	Integrating child rights considerations into all appropriate corporate policies and management processes	Appoint a designated individual or team responsible for this process, granting them access to both internal and external stakeholders. Empower this person or team to lead efforts to prioritize child online protection within the company. Develop a comprehensive child protection and safeguarding policy or incorporate specific considerations related to children and young people's rights into broader company policies, such as those related to human rights, privacy, marketing, and relevant codes of conduct. Integrate assessments of child online protection issues into existing frameworks for assessing human rights or risks, whether at the corporate level, product or technology level, or within specific countries. This helps determine if the company's activities, products, services, or business relationships may be causing or contributing to negative impacts on children's rights. Identify the impacts on children's rights across different age groups resulting from company operations, as well as from the design, development, and launch of products and services. Additionally, identify opportunities to actively support the rights of children and young people. Adopt an approach that empowers and educates children for protection. Keep in mind their rights regarding data protection, privacy, and freedom of speech while delivering education and guidance through the company's services. Leverage both internal and external expertise and engage with key stakeholders, including children and young people, to seek continuous feedback and guidance on child online safety measures and company strategies. In regions where legal frameworks for safeguarding children and young people's rights to privacy and freedom of expression are lacking, ensure that company policies and practices adhere to international standards, such as those outlined in the United Nations General Assembly Resolution 68/167 addressing privacy rights in the digital age. Establish operational-level grievance and reporting mechanisms to address child rights violations, including cases involving child sexual abuse material (CSAM), inappropriate content, unwanted contact, or breaches of privacy. Designate a child protection policy manager or a designated point of contact for child online protection issues. In situations where a child is at risk of harm, the child protection policy manager should promptly notify the appropriate authorities. Public service media, like the BBC, have set guidelines mandating the appointment of a child protection policy manager as a standard practice.
2	Developing industry standards to protect children online	Develop and put into effect standards at both the company and industry levels to safeguard the rights of children and young individuals, tailoring them to the unique characteristics of the industry and its features.

3	Developing standard processes to CSAM	Establish internal procedures to ensure compliance with local and international laws in the fight against CSAM. Create a senior-level position or team within the organization responsible for integrating these procedures. Industry members should report the actions and outcomes achieved by this team in their annual corporate and sustainability reports. When national regulations fall short in providing adequate protection, companies should not only comply with but also surpass national legislation. They should leverage their influence to advocate for legislative changes that empower the industry to combat CSAM. A dedicated senior position or team should oversee the integration of these procedures and monitor operations. These efforts should be transparently disclosed in the annual corporate and sustainability reports, accessible to the public. Specify the company's commitment to full cooperation with law enforcement investigations in cases of reported or discovered illegal content. Outline the penalties, such as fines or cancellation of billing privileges, for misuse of services to store or share CSAM in customer terms and conditions or acceptable use policies. Develop notice and takedown processes and reporting mechanisms that enable users to report CSAM or inappropriate contact, including details about the specific profile or location where it was encountered. Establish procedures for following up on reports, capturing evidence, and promptly removing or blocking access to CSAM. When necessary, seek expert opinions, such as from national COP bodies, before deleting illegal content. Ensure that any third parties with whom the company has contractual relationships also have robust notice and takedown processes in place. Be prepared to handle CSAM cases and report them to relevant authorities. If no prior relationship exists with law enforcement and national hotlines, collaborate with them to develop processes jointly. Work with internal departments like customer care, fraud prevention, and security to enable the business to submit reports of suspected illegal content directly to law enforcement and hotlines. Implement policies or programs to support the well-being and safety of staff who may be exposed to harmful content, ensuring their resilience and minimizing potential harm. Incorporate data retention and preservation policies to support law enforcement during criminal investigations, ensuring the capture of evidence. Document the company's procedures for managing CSAM, from monitoring to content transfer and destruction, including a list of personnel responsible for handling the material. Encourage the reporting of CSAM by implementing accessible reporting mechanisms and ensuring that customers are aware of how to report such content. If a national hotline is available, provide links to it on the corporate website and relevant content services promoted by the company. Take necessary measures across all services and data sets to prevent the dissemination of known child sexual abuse content on the company's services or platforms. Regularly assess all content hosted on the company's servers, including commercial content from third-party providers, using tools like hash scanning for known child sexual abuse images, image recognition software, or URL blocking to address CSAM effectively.

4	Creating a safer and age- appropriate online environment	Ensure that content and services unsuitable for users of all ages are managed as follows: Classify such content in accordance with national standards and cultural norms. Align with existing standards established in equivalent media. Provide clear and prominent options for controlling access to such content. Offer age verification where appropriate, along with transparent terms regarding the removal of any personally identifiable data collected during the verification process. For instance, media regulatory authorities, including organizations like Ofcom in the United Kingdom, CSA in France, and AGCOM in Italy, lay out requirements for age-related content, and Internet providers must adapt their content offerings to comply with these guidelines. Implement clear reporting tools and establish a follow-up process for addressing reports of inappropriate content, contact, and misuse. Furnish detailed feedback to service users regarding the reporting procedure. Conduct pre-moderation of interactive spaces designed for children and young people in a manner consistent with children's rights to privacy and their evolving capabilities. Proactive moderation can help create an environment where bullying and harassment are not tolerated. Unacceptable behaviors encompass actions such as posting threatening comments on someone's profile, creating fake profiles or hate sites to shame a victim, sending harmful chain messages and attachments, or hacking into someone's account to send offensive messages. Exercise particular caution with staff members or collaborators who work with children and young people. It may be necessary to conduct background checks, including criminal record checks with law enforcement authorities. Promptly report any suspected grooming incidents to the online or interactive executive management team responsible for notifying the appropriate authorities. Enable users to directly report suspected grooming incidents to the authorities and establish contact options, such as email addresses, for alerts and reporting. Always prioritize the safety and well-being of the child, ensuring that all interactions with children are essential to the service, program, event, activity, or project. Never assume sole responsibility for a child; if a child requires care, inform the parent, guardian, or chaperone. Listen to and respect children at all times. If anyone exhibits inappropriate behavior around children, report such behavior to the local child protection contact. Establish a well-defined set of rules that are prominently displayed and reflect key points from the terms of service and acceptable use guidelines. Use user-friendly language to clarify: • The service's nature and user expectations. • What is deemed acceptable and unacceptable in terms of content, conduct, and language, with a clear prohibition of illegal activities. • Appropriate consequences for breaches, such as reporting to law enforcement or account suspension. Facilitate customer reporting of concerns related to misuse through accessible and standardized processes, particularly for issues like receiving unwanted communications (e.g., spam SMS). Provide transparent information to customers regarding the services offered, including: • Content or service type and associated costs. • Minimum age requirements for access. • Availability and coverage of parental controls (e.g., network-level controls) and guidance on their utilization. • Details about the collection and use of user information. Promote national support services that allow children and young people to report incidents and seek assistance in cases of abuse or exploitation, such as those offered by organizations like Child Helpline International.

	Educating children, parents and educators about children's safety and their responsible use of ICTs	Industry can enhance technical measures with educational and empowerment initiatives through these steps: Clearly articulate the available content and associated parental controls or family safety settings. Ensure that language and terminology are easily understandable, prominently displayed, and relevant for all users, including children, parents, and caregivers. This applies to aspects like terms and conditions, service costs, privacy policies, safety guidelines, and reporting procedures. Educate customers on effectively managing concerns related to Internet usage, covering issues like spam, data security, and inappropriate interactions such as cyberbullying and grooming. Provide information on the actions users can take and how to report inappropriate activities. Establish mechanisms and educate parents about participating in their children's online activities, especially younger children. This may include enabling parents to review and adjust the privacy settings of their children. Collaborate with government authorities and educational institutions to empower parents with the skills and knowledge needed to guide their children and young people in becoming responsible digital citizens and proficient ICT users. In accordance with the local context, offer educational resources suitable for both school and home use to enhance children and young people's ICT skills and foster critical thinking. These materials should empower them to use ICT services safely and responsibly. Assist customers by distributing family online safety guidelines, encouraging parents and caregivers to: Familiarize themselves with the products and services their children and young people are using. Ensure that children and young people use electronic devices in moderation as part of a healthy and balanced lifestyle. Vigilantly observe changes in the behavior of children and young people to identify potential signs of cyberbullying or harassment. Equip parents with the necessary information to comprehend their children's use of ICT services, effectively address concerns related to harmful content and behavior, and be prepared to guide their children in responsible usage. Collaboration with school districts can facilitate the provision of online safety curricula for children and educational materials for parents.
	Using technology advances to protect and educate children	AI technologies that prioritize privacy can analyze text, images, conversations, and contexts to identify and tackle various online dangers and risks. This information can then be leveraged to educate and empower children in dealing with these issues. When these processes occur within a smart device ecosystem, it ensures the protection of young people's data and privacy while still providing support. Public service and national media have a crucial role to play in their program offerings, both offline and online, by educating parents and children and raising their awareness about the advantages and hazards of the online environment.

	Promoting digital technology as a mode to further civic engagement	Industry can promote and enable the involvement of children and young people by taking the following steps: Offer information about a service that emphasizes the advantages children can enjoy by using it responsibly and positively, such as for creative endeavors. Put in place documented procedures to ensure the consistent enforcement of policies and processes that safeguard freedom of expression for all users, including children and young people. Prevent excessive blocking of legitimate and age-appropriate content. To ensure that filtering requests and tools are not misused to restrict children and young people's access to information, maintain transparency regarding blocked content and establish a reporting process for users, including webmasters, to report any unintended blocking. This reporting process should be accessible to all users and include clear, responsible, and well-defined terms of service. Develop online platforms that champion children and young people's right to express themselves, promote their participation in public life, and encourage their involvement in collaborative, entrepreneurial, and civic activities. Create educational content for children and young people that fosters learning, creative thinking, and problem-solving skills. Support digital literacy, capacity building, and ICT skill development to empower children and young people, particularly those in rural and underserved areas, to effectively use ICT resources and participate safely in the digital realm. Collaborate with local civil society organizations and government agencies to address national and local priorities for expanding universal and equitable access to ICTs, platforms, devices, and the necessary infrastructure. Inform and engage customers, including parents, caregivers, children, and young people, about the services provided. This should include details about the types of content available, corresponding parental controls, reporting mechanisms for abuse or inappropriate content, follow-up procedures for reports, age-restricted services, and guidance on safe and responsible usage of interactive services provided by the company. Address broader issues related to safe and responsible digital citizenship, such as online reputation, digital footprint, harmful content, and grooming. Consider partnering with local experts, such as children's NGOs, charitable organizations, and parenting groups, to shape the company's messaging and effectively reach the target audience. If the company already collaborates with children or schools through corporate social responsibility programs, explore opportunities to expand this engagement to include educating and engaging with children, young people, and educators on child online protection (COP) messages.
	Investing in research	Allocate resources to support research and comprehensive analysis of digital technologies, their effects on children, and the considerations related to child protection and child rights in the digital landscape. This investment aims to incorporate online protection mechanisms into services that children and young people use while gaining insights into the most impactful interventions for enhancing children's online experiences.

Typology of ICT companies

While these guidelines are primarily aimed at the ICT industry as a whole, it's important to recognize that technology companies vary significantly in terms of the services they provide, their operational methods, the regulations they adhere to, and the scale of their offerings. Any tech company that offers products or services intended for children, whether directly or indirectly, can benefit from the overarching principles outlined earlier. They can adapt these principles based on their specific areas of operation. The fundamental idea is to assist and direct the ICT industry in taking appropriate measures to enhance online child protection, mitigating potential risks, while also empowering children to navigate the digital realm effectively. The following typology offers a clearer insight into some of the target audiences and their alignment with the checklists in the subsequent sections. It's important to note that these are just a few specific categories and do not cover all possibilities:

a. Internet service providers, which encompass fixed landline broadband services and mobile network operators' cellular data services. This may also extend to businesses that provide public Wi-Fi hotspots, whether free or paid.

b. Social networking and messaging platforms, as well as online gaming platforms.

c. Manufacturers of hardware and software, including providers of handheld devices like mobile phones, gaming consoles, voice-activated home devices, Internet of Things products, and smart toys connected to the Internet for children.

d. Companies involved in digital media, such as content creators, those offering access to content, and content hosting providers.

e. Companies providing streaming services, including live streaming platforms.

f. Companies that offer digital file storage services and cloud-based solutions.

FEATURE-SPECIFIC CHECKLISTS[24]

This section serves as an extension to the earlier general industry checklist, offering tailored recommendations for companies that provide services with specific features aimed at respecting and upholding children's online rights. These feature-specific checklists provide additional guidance that complements the overarching principles and strategies presented in Table 1. Therefore, companies should consider these feature-specific checklists in conjunction with the steps outlined in Table 1.

The highlighted features in these checklists are multifaceted, and several of them may be applicable to the same company. The subsequent feature-specific checklists are categorized in alignment with the key areas covered in the general guidelines presented in Table 1. Each of these feature-specific checklists has been developed collaboratively with key contributors, resulting in slight variations among them.

Feature A: Provision of Connectivity, Data Storage, and Hosting Services

Access to the Internet is a crucial element for the fulfillment of children's rights, as it can open up vast opportunities and resources for them. Companies that offer connectivity, data storage, and hosting services have a significant role in integrating safety and privacy measures into their services, especially for children and young people. This specific service feature encompasses various entities, including mobile operators, Internet service providers, data storage systems, and hosting service providers.

[24] ITU Publications, 2020, Guidelines for Industry on Child Online Protection. http://handle.itu.int/11.1002/pub/81598fd4-en

Mobile operators play a pivotal role by facilitating Internet access and offering a variety of mobile-specific data services. Many of these operators have already committed to Codes of Practice for Child Online Protection (COP) and provide tools and educational materials to uphold their responsibilities.

Internet service providers serve as intermediaries, providing Internet access and acting as repositories for data through their hosting, caching, and storage services. Consequently, they bear a primary responsibility for safeguarding children's online experiences.

Internet Access in Public Spaces

It is becoming increasingly common for various entities like municipalities, retailers, transportation companies, hotel chains, and other businesses and organizations to offer Internet access through Wi-Fi hotspots. Often, this access is provided for free or at a minimal cost, sometimes with minimal sign-up requirements, either as a public service or to attract customers to their locations and services.

Promoting the availability of Wi-Fi is an effective way to ensure Internet connectivity in specific areas. However, caution must be exercised when providing such access in public spaces where children are likely to be present regularly. Users should be aware that Wi-Fi signals may be accessible to passers-by, potentially compromising user data security. As a result, Wi-Fi providers may not always be able to monitor or supervise the usage of the Internet connection they offer. Users, especially parents and guardians, should take precautions not to share sensitive or personal information when using publicly available Wi-Fi.

In public spaces, Wi-Fi providers may want to consider additional measures to safeguard children and young people. These measures could include:

- Actively blocking access to web addresses known to contain inappropriate content for a broad audience, in addition to their efforts to block access to child sexual abuse material (CSAM).
- Including clauses in the terms and conditions of Wi-Fi use that prohibit accessing or displaying any material unsuitable for an environment where children are present. These terms and conditions should also outline clear consequences for violations of such rules.
- Implementing robust security measures to protect against unauthorized access, which could lead to the manipulation or loss of personal data.
- Employing filters on the Wi-Fi system to reinforce the policy against inappropriate content.
- Providing procedures and software to offer optional parental control features related to children and young people's access to Internet content.

Best Practices: In several European Union member states, telecommunication regulations mandate that network access be identified through individual SIM cards or other identification tools.

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

Sl. No.	Key Areas for consideration	Description
	Integrating child rights considerations into all appropriate corporate policies and management processes	Providers offering connectivity, data storage, and hosting services have the capacity to recognize, forestall, and alleviate the negative consequences of information and communication technologies (ICTs) on the rights of children and young individuals. They can also pinpoint prospects for fostering the progress of children and young people's rights. Please consult the overarching recommendations outlined in Table 1 for further guidance.
	Developing standard processes to handle CSAM	In cooperation with government agencies, law enforcement, civil society groups, and hotline organizations, providers of connectivity, data storage, and hosting services can have a significant role in combatting Child Sexual Abuse Material (CSAM). Here are the steps they can take: Collaborate with government bodies, law enforcement agencies, civil society organizations, and hotline entities to effectively address CSAM issues and report relevant cases to the appropriate authorities. If there's no existing relationship with law enforcement or hotlines, engage in cooperative efforts to establish efficient procedures. Offer ICT training to law enforcement personnel to enhance their capabilities in handling CSAM cases. In regions where legal and law enforcement oversight concerning CSAM is less developed, direct individuals seeking to report such cases to the International Association of Internet Hotlines (INHOPE), where they can submit reports to international hotlines. Consider implementing globally recognized URL or website blocking lists, which are curated by relevant authorities (e.g., national law enforcement agencies, hotlines, Cybertip Canada, Interpol, IWF). This approach can make it more challenging for users to access identified CSAM. Develop processes for reporting, notice, and takedown procedures. Establish a public service agreement outlining the response protocol and the timeframe for content removal. You may refer to resources like the UNICEF and GSMA Guide on notice and takedown policies and practices. Create a reporting mechanism with clear instructions on how to use it. Provide guidance on the types of illegal content and conduct to report, and specify which materials should not be attached with the report to prevent further dissemination on the Internet. These actions can contribute significantly to addressing CSAM and promoting online safety for children and young people. Assist law enforcement in criminal investigations by helping gather evidence. Explicitly prohibit the use of services to store, share, or distribute Child Sexual Abuse Material (CSAM) in the terms of service and conditions. Ensure that these terms clearly communicate a zero-tolerance policy toward CSAM. Clearly state in the terms of service and conditions that the company will fully cooperate with law enforcement investigations when CSAM is discovered or reported. At the national level, there are two primary reporting solutions for CSAM online: hotlines and reporting portals. An up-to-date list of all existing hotlines and portals can be found at INHOPE. Hotlines: If there isn't a national hotline available, explore options to establish one, which can be achieved through various means, including collaboration with INHOPE and the INHOPE Foundation. Refer to the GSMA INHOPE Hotlines Guide for comprehensive guidance, and use the interactive version of the guide to help customer care staff report questionable content to law enforcement and INHOPE effectively. Reporting portals: The IWF offers a reporting portal solution that enables Internet users in countries without hotlines to directly report suspected child sexual abuse images and videos to the IWF through a dedicated online portal page. For providers of connectivity, data storage, and hosting services involved in content hosting (not all are), it is essential to have established notice and take-down processes in place.

	Creating a safer and age-appropriate digital environment	Providers of connectivity, data storage, and hosting services can contribute to a safer and more enjoyable digital environment for children of all ages by taking the following steps: Data storage and hosting service providers should ensure that the reporting function is prominently displayed on all web pages and services. They should also establish clear and documented procedures for promptly addressing reports of abuse or violations of terms and conditions. Connectivity providers should either offer their own user-friendly technical controls or guide users to tools developed by specialized providers. These tools should be suitable for the services offered and easy for end-users to implement. Additionally, they should enable users to block or filter Internet access through the company's networks. If the company provides content or services, including those from third-party providers promoted by the company, that are intended exclusively for adult users (such as certain games or lotteries), appropriate age-verification mechanisms should be implemented.
	Educating children, parents and educators about children's safety and their responsible use of ICTs	Providers of connectivity, data storage, and hosting services should convey key messages from their terms and conditions in user-friendly community guidelines to assist children and their parents and caregivers. They should also integrate reminders within the service itself, especially during content uploads, regarding inappropriate content. Additionally, service providers should furnish children and young people with guidance on safe Internet usage. They can explore innovative ways to communicate important messages, such as: "Never disclose any personal information, like your address or phone number, to individuals you haven't met in person." "Always consult with an adult before planning to meet someone you've connected with online. Inform a trusted friend about your plans." "Don't respond to bullying, offensive, or obscene messages. Instead, save the evidence and refrain from deleting the messages." "If something or someone makes you uncomfortable or upset online, confide in a trusted adult or friend." "Guard your account password and username carefully. Be cautious, as some online users may provide false information to persuade you to share personal details." Service providers can collaborate with organizations experienced in educating and supporting children in safe Internet practices. Resources like the Child Helpline International and GSMA's practical guide can offer valuable insights into these partnerships.
	Promoting digital technology as a mode to further civic engagement	Refer to the general guidelines in Table 1.

Feature B: Offer curated digital content

The Internet hosts a wide range of content and activities, including those specifically designed for children and young individuals. Companies that provide services with curated content have significant opportunities to prioritize safety and privacy for these audiences. This service aspect encompasses businesses involved in developing their own content as well as those granting access to digital content. It pertains to various sectors, including news and multimedia streaming services, national and public service broadcasting, and the gaming industry.

Table 3 offers recommendations to guide providers of services that curate content on the policies and steps they can implement to improve child online protection and engagement.

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

Sl. No.	Key Areas for consideration	Description
1	Integrating child rights considerations into all appropriate corporate policies and management processes	Services that offer curated digital content can contribute to protecting and promoting the rights of children and young individuals by implementing the following measures: Establish policies that prioritize the well-being of children and young people who engage in online content creation. These policies should encompass the physical and emotional welfare and dignity of individuals under 18 participating in programs, movies, games, news, etc., regardless of any consent provided by a parent or guardian.
2	Developing standard processes to handle CSAM	In collaboration with government entities, law enforcement agencies, civil society organizations, and hotline providers, companies that offer curated digital content can actively contribute to the fight against CSAM through the following actions: In instances involving CSAM, particularly when users can upload content through features like "comments" or "reviews," company staff should promptly engage with the executive management team responsible for reporting such materials to the appropriate authorities. They should also take the following steps: • Immediately notify national law enforcement agencies. • Inform their immediate supervisor and report the content to the child protection policy manager. • Reach out to the internal investigation service via phone or email, providing incident details and seeking guidance. • Await instructions from the relevant agency before taking action, which may involve deleting the material, storing it in a shared location, or forwarding it as directed.
3	Developing standard processes to handle CSAM	If any such material is identified, it should be promptly reported to a specialized organization dedicated to online safety. This organization typically operates a hotline where members of the public and IT professionals can report specific instances of potentially illegal online content. For instance, following its Child Protection and Safeguarding Policy, the BBC has issued editorial guidance regarding interactions with children and young individuals on the Internet. Additionally, they have developed supplementary checklists and codes of conduct for working with children and young people online, which extend to subcontractors and external providers. In the United Kingdom, Ofcom has separate policies on child protection that address online content, mobile devices, and game consoles. To effectively address situations involving CSAM or suspected illegal activities, it's essential to implement a swift and robust escalation strategy. To achieve this: • Provide users with a straightforward and easily accessible means of reporting violations of community rules. • Remove content that violates these rules. Before uploading age-sensitive curated content to a social networking platform, it's important to be aware of and adhere to the site's terms and conditions, taking into account the minimum age requirements specified on different social networking platforms. Furthermore, the terms and conditions for each online platform should include clear mechanisms for reporting any breaches of these rules.

4	Creating a safer and age-appropriate online environment	Companies offering curated digital content can contribute to creating a safer and more enjoyable digital environment for children and young people across various age groups by taking the following actions: Collaborate with industry peers to establish content classification and age rating systems that adhere to recognized national or international standards. These systems should maintain consistency across different media platforms. For example, a movie trailer in a cinema and on a smartphone should display the same age classifications. Develop child-friendly and age-appropriate products with built-in safety features and robust age-verification systems. Align applications and services across different media with content rating systems to assist parents and caregivers in making informed decisions about content appropriateness for children and young people. Implement effective age-verification methods to prevent children and young people from accessing content, websites, products, or interactive services intended for older age groups. Provide users with guidance and reminders regarding the nature and age classification of the content they are accessing. For audiovisual and multimedia service providers, consider issuing personal identification numbers to users seeking access to potentially harmful content for children and young people. Ensure transparency in pricing for products and services, as well as in data collection practices. Compliance with relevant privacy laws pertaining to children and young people's privacy, including parental consent for data collection, should be maintained. Clearly distinguish advertising or commercial communication from other content. Monitor online content and tailor it to the expected user audience. Establish user-friendly policies, especially for online interactions such as commenting, forums, social networks, gaming platforms, chat rooms, or message boards, and include them in terms of service and user guidelines. Determine the desired level of engagement before launching an online service. Services targeting children should exclusively present content suitable for young audiences. Consult with relevant national authorities responsible for child protection if uncertainties arise. Provide accurate and clear content labels. Be aware that users can access inappropriate content by following links on third-party sites that bypass contextualizing pages.

5	Educating children, parents and educators about children's safety and their responsible use of ICTs	Companies offering curated digital content can contribute to creating a safer and more enjoyable digital environment for children and young people across various age groups by taking the following actions: Collaborate with industry peers to establish content classification and age rating systems that adhere to recognized national or international standards. These systems should maintain consistency across different media platforms. For example, a movie trailer in a cinema and on a smartphone should display the same age classifications. Develop child-friendly and age-appropriate products with built-in safety features and robust age-verification systems. Align applications and services across different media with content rating systems to assist parents and caregivers in making informed decisions about content appropriateness for children and young people. Implement effective age-verification methods to prevent children and young people from accessing content, websites, products, or interactive services intended for older age groups. Provide users with guidance and reminders regarding the nature and age classification of the content they are accessing. For audiovisual and multimedia service providers, consider issuing personal identification numbers to users seeking access to potentially harmful content for children and young people. Ensure transparency in pricing for products and services, as well as in data collection practices. Compliance with relevant privacy laws pertaining to children and young people's privacy, including parental consent for data collection, should be maintained. Clearly distinguish advertising or commercial communication from other content. Monitor online content and tailor it to the expected user audience. Establish user-friendly policies, especially for online interactions such as commenting, forums, social networks, gaming platforms, chat rooms, or message boards, and include them in terms of service and user guidelines. Determine the desired level of engagement before launching an online service. Services targeting children should exclusively present content suitable for young audiences. Consult with relevant national authorities responsible for child protection if uncertainties arise. Provide accurate and clear content labels. Be aware that users can access inappropriate content by following links on third-party sites that bypass contextualizing pages.
6	Promoting digital technology as a mode to further civic engagement	Companies providing curated digital content can promote and enable the participation of children and young people by taking the following actions: Create and provide a diverse selection of high-quality content that is engaging, educational, and age-appropriate. This content should help children and young people better understand their surroundings and contribute to their physical, mental, and social development. It should not only be visually appealing and user-friendly but also safe and dependable. Encourage the development and promotion of content that empowers children to embrace diversity and become positive role models.

Feature C: Host user-generated content and connect users

There was a time when adults dominated the online world, but it's now evident that children and young people play a significant role across various platforms, actively creating and sharing user-generated content. This service feature pertains to various platforms, including social media services, apps, and websites focused on creative expression.

Services that facilitate user connections can be categorized into three main groups:

1. Primarily messaging apps (e.g., Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp).
2. Primarily social networking services that host user-generated content, allowing users to share and connect both within and beyond their networks (e.g., Instagram, Facebook, Snapchat, TikTok).
3. Primarily live streaming apps (e.g., Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

These service providers typically set a minimum age requirement for user sign-ups, although enforcing this age verification can be challenging since it relies on users' self-reported ages. Furthermore, many of these services allow location-sharing features, which can make children and young people more vulnerable to offline risks.

Table 4, adapted from guidelines used by one of the largest social networks, offers recommendations for service providers hosting user-generated content and connecting new users to enhance child online protection and support children's participation.

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

Sl. No.	Key Areas for consideration	Description
1	Integrating child rights considerations into all appropriate corporate policies and management processes	Platforms that host user-generated content and facilitate user connections can play a crucial role in safeguarding children and young people's rights in the digital realm, as well as in promoting and enhancing these rights. Please consult the overarching guidelines provided in Table 1 for more details.
2	Developing standard processes to handle CSAM	In collaboration with government authorities, law enforcement agencies, civil society organizations, and hotline initiatives, companies that host user-generated content and facilitate user connections can actively contribute to combating CSAM through the following measures: Establish clear procedures for all platforms to promptly assist law enforcement during both emergency situations and routine inquiries. Explicitly state the commitment to full cooperation with law enforcement investigations if illegal content is reported or discovered, and outline potential penalties, such as fines or the cancellation of billing privileges. Collaborate with internal departments like customer care, fraud prevention, and security to enable the reporting of suspected illegal content directly to law enforcement and hotlines. Ensure that frontline staff are shielded from exposure to harmful content and consider implementing support programs to protect their well-being and resilience. Use terms of service and conditions to explicitly prohibit illegal content and behaviors, emphasizing that harmful content, including suspected grooming of children for contact or non-contact abuse, and illegal content, such as CSAM, will not be tolerated. Highlight the commitment to refer and collaborate with law enforcement in cases of illegal content or any breaches of the child protection policy. Document the company's practices for handling CSAM comprehensively, from monitoring to the final disposal of the content. Maintain a record of personnel responsible for managing such material. Implement policies regarding the ownership of user-generated content, including the option to remove user-created content upon request. Remove content that violates platform policies and inform the user responsible for the violation. Clearly communicate to users that non-compliance with acceptable use policies will result in various consequences, which may include: 1. Removal of their content. 2. Suspension or closure of their account. 3. Revocation of their ability to share specific types of content or use certain features. 4. Restrictions on their ability to contact children. 5. Referral of the matter to law enforcement authorities.

3	Developing standard processes to handle child sexual abuse material	Encourage users to report CSAM or any other illegal content and ensure that customers are aware of the reporting process in place if they come across such material. Establish systems and employ trained staff to evaluate incidents on a case-by-case basis and take appropriate actions. Create comprehensive and well-funded user support teams capable of handling various types of incidents to ensure suitable responses and actions. When a user submits a complaint, route it to the appropriate staff based on the nature of the incident. Consider setting up specialized teams to handle user appeals in cases where reports may have been filed incorrectly. Implement processes for the immediate removal or blocking of access to CSAM, including notice and takedown procedures to swiftly eliminate illegal content upon identification. Comply with legislation that allows for the preservation of such material as evidence in criminal investigations. Develop technical systems capable of detecting known illegal content and preventing its upload, including within private groups, or flagging it for prompt review by the company's safety team. Take all necessary measures to safeguard services against misuse for hosting, disseminating, or creating CSAM. When feasible, employ proactive technical measures to analyze objects and metadata associated with user profiles to detect criminal behavior or patterns and take appropriate action. If the application or service permits users to upload and store images on servers owned or operated by the company, establish processes and tools to identify images likely to contain CSAM. Consider proactive identification techniques, such as scanning technology or human review.

4	Creating a safer and age-appropriate online environment	Service providers offering user-generated content and facilitating user connections can contribute to a safer and more enjoyable digital environment for children of all ages by taking the following actions: Clearly communicate a set of "house rules" within the terms of service and user guidelines in user-friendly language, defining: • The nature of the service and user expectations. • Acceptable and unacceptable content, behavior, and language, explicitly prohibiting illegal usage. • Consequences for any breaches, such as reporting to law enforcement or suspension of user accounts. Present key safety and legal messages in an age-appropriate format, using intuitive icons and symbols, during sign-up and as different actions are taken on the platform. Simplify the process for customers to report concerns about misuse to customer support, providing standard and accessible procedures for addressing various concerns, including issues like spam, bullying, or inappropriate content. Offer age-appropriate content-sharing and visibility settings, defaulting to more restrictive privacy and visibility settings for children and young people compared to adults. Enforce minimum age requirements and explore the development of new age-verification systems, such as biometrics, adhering to established international standards for their creation. Take measures to identify and remove underage users who have misrepresented their age to gain access, considering the collection, storage, and processing of additional personal data that this may entail. Establish a reporting function or help center to encourage users to report individuals who have falsified their ages. Ensure the protection of younger users from unsolicited communication and establish robust privacy and information-collection guidelines. Implement methods for reviewing hosted images and videos to promptly remove inappropriate content upon detection. Utilize tools like hash scanning for known images and image recognition software. In services aimed at children, take proactive measures to check photos and videos before publication to prevent the sharing of sensitive personal information. Implement various measures to control access to user-generated content and safeguard children and young people from inappropriate or illegal content in online environments. Promote the use of secure passwords to enhance protection, particularly in gaming and social media settings. Additional techniques include: • Conducting reviews of discussion groups to identify harmful topics, hate speech, and illegal activities, and promptly deleting such content that violates terms of use. • Developing tools to actively search for and remove illegal or rule-violating content from the platform, along with mechanisms to prevent the uploading of known illegal material. • Implementing pre-moderation of message boards by specialized moderators focused on children and young people, who review content for compliance with established "house rules." Each message can undergo scrutiny before publication, and moderators can identify and flag suspicious or distressed users. • Establishing a team of community hosts who serve as the initial point of contact for moderators when concerns arise regarding a user. Take responsibility for reviewing commercial content across forums, social networks, and gaming platforms. Implement appropriate standards and rules to shield children from age-inappropriate advertising and set clear boundaries for online advertising directed at children and young people.

5	Educating children, parents and educators about children's safety and their responsible use of ICTs	Service providers offering user-generated content can enhance technical measures with educational and empowerment initiatives through the following actions: Establish a dedicated section featuring safety tips, articles, interactive content about digital citizenship, and links to valuable resources from trusted experts. Ensure that safety advice is prominently displayed and presented in user-friendly language. Maintain a consistent navigation interface across various devices for user convenience. Provide parents with clear information about the available content and services, including explanations of concepts like social networking sites, location-based services, mobile Internet access, and parental control options. Educate parents on how to report instances of abuse, misuse, or inappropriate/illegal content and outline the reporting process. Inform them about age restrictions on certain services and promote safe and responsible behavior when using interactive platforms. Implement a "trust and reputation" system to incentivize positive behavior and encourage users to set good examples for one another. Emphasize the significance of social reporting, allowing individuals to seek assistance from other users or trusted friends in resolving conflicts or addressing concerning content. Offer guidance and reminders regarding the nature of specific services or content and how to enjoy them safely. Incorporate community guidelines into interactive services, including safety pop-ups that remind users of appropriate and secure conduct, such as refraining from sharing personal contact details. Collaborate with parents to ensure that information shared about children on the Internet does not expose them to risks. Seek informed consent from children whenever possible when featuring them in user-created content and respect their decisions in this regard.
6	Promote digital technology as a mode to further civic engagement	Services that host user-generated content can promote and empower children and young people to exercise their right to participation by following the general guidelines outlined in Table 1.

Feature D: Artificial intelligence-driven systems

The terms "artificial intelligence," "machine learning," and "deep learning" have been used interchangeably by the general public to describe the idea of replicating intelligent behavior in machines. This section focuses on the impact of machine learning and deep learning processes on children's lives and their human rights.

Due to the rapid advancement of artificial intelligence-based technologies in recent years, the current international framework for protecting children's rights does not explicitly address many issues raised by the development and use of artificial intelligence. However, it does identify several rights that may be affected by these technologies, including the rights to privacy, education, play, and non-discrimination[25].

The application of AI can affect children's experiences with various services used on social networks, such as video streaming platforms. Popular video-sharing platforms use machine-learning algorithms in their recommendation engines to optimize views of specific videos (footnote 24). These platforms are accessible to very young children, and there is concern that recommendation algorithms can expose children to inappropriate content and create "filter bubbles" that limit their exposure to child-friendly programming (footnote 24).

AI also impacts child online protection, particularly with smart toys. Smart toys involve multiple processes, including the toy itself, a mobile application acting as a Wi-Fi access point, and an online account where data is stored. These toys communicate with cloud-based servers, raising privacy concerns if security measures are not applied at every layer. Instances of hacking have resulted in the leakage of personal details, and some hacked devices can be used for unauthorized surveillance.

When implementing response mechanisms to detect threats against children using these devices, it is crucial that companies base their recommendations on evidence and consult with child protection and safeguarding experts.

While some companies are developing ethical principles for the use of AI[26], there is a lack of clear public policies regarding AI and children[27]. Various technology and trade associations, as well as computer science groups, have drafted ethical principles related to AI[28], but these principles do not explicitly address child rights, the risks AI technologies pose to children, or proactive measures to mitigate these risks.

"Similar to businesses, governments worldwide have implemented strategies aimed at positioning themselves as pioneers in AI development and utilization, creating favorable conditions for innovators and corporations. Nevertheless, it remains unclear how these national strategies specifically consider the rights of children." (footnote 27)

Improving Facebook's handling of suicide and self-injury-related content: In 2019, Facebook initiated regular consultations with global experts to address challenging issues related to suicide and self-injury content. These discussions covered topics like handling suicide notes, the risks associated with depressive content online, and the portrayal of suicide in the news. Detailed information about these meetings is accessible on Facebook's new Suicide Prevention page within its Safety

[25] UNICEF and UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.
[26] See Microsoft, "Salient Human Rights Issues", Report - FY17; and Google, "Responsible Development of AI" (2018).
[27] Microsoft Official Blog, "The Future Computed: Artificial Intelligence and its role in society", 2018.
[28] The Guardian, "'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft", 2016.

Center. These consultations led to several enhancements in how Facebook manages such content. For instance, policies regarding self-harm were reinforced to prohibit the display of graphic images depicting cutting, in order to prevent unintentional promotion or triggering of self-harm. Even when individuals are seeking support or expressing themselves to aid their recovery, Facebook now places a sensitivity screen over images of healed self-harm wounds. This content is now detected through AI, enabling automatic actions, including removal or the addition of sensitivity screens, to be taken on potentially harmful content. From April to June 2019, Facebook addressed over 1.5 million pieces of suicide and self-injury content on its platform, with more than 95 percent of it being identified before user reports. During the same period, Instagram dealt with over 800 thousand pieces of similar content, of which over 77 percent was detected prior to user reporting.

Identifying potential bullying or peer-to-peer violence in real time and messaging users: Instagram is implementing artificial intelligence (AI) to identify and address behaviors like insults, shaming, and disrespect. This involves employing advanced reporting tools, which enable moderators to promptly suspend the account of individuals engaged in online bullying.

Good practice: Use artificial intelligence in the identification of child sexual abuse material: Facebook has developed advanced technologies, including PDQ and TMK+PDQF, to identify and combat child sexual abuse content. These technologies are part of a broader suite of tools used by Facebook to detect harmful content. Other algorithms and tools used in the industry include pHash, aHash, and dHash. While PDQ drew inspiration from pHash, it was built as a separate algorithm with independent software implementation. The video-matching technology, TMK+PDQF, was a collaborative effort between Facebook's AI Research team and academics from the University of Modena and Reggio Emilia in Italy.

These technologies allow for efficient storage of files as short digital hashes, enabling the determination of whether two files are the same or similar, even without access to the original image or video. These hashes can also be easily shared with other companies and non-profit organizations. PDQ and TMK+PDQF are designed to operate at a large scale, supporting video-frame hashing and real-time applications.

Table 5. COP checklist for Feature D: AL-driven systems

Sl. No.	Key Areas for consideration	Description
1	Integrating child rights considerations into all appropriate corporate policies and management processes	Providers of AI-driven systems can play a role in safeguarding and promoting the rights of children and young people while also identifying ways to advance those rights. AI systems should be designed, developed, implemented, and researched with a commitment to upholding the rights outlined in the Convention on the Rights of the Child, recognizing that childhood increasingly involves digital experiences that require special care and support. When creating products or services for children, an inclusive design approach should be employed, considering gender, cultural, and geographic diversity. This approach should involve input from various stakeholders, including parents, teachers, child psychologists, and, when appropriate, children themselves. To ensure that AI systems do not violate child rights, governance frameworks, ethical guidelines, laws, standards, and regulatory bodies should be established to oversee the application of AI technologies. These measures are essential to protect and support the rights of children in the digital age.
2	Developing standard processes to handle CSAM	Collaborating with government, law enforcement, civil society, and hotline organizations, AI-driven system providers can actively contribute to the fight against CSAM by following the general recommendations outlined in Table 1.
3	Creating a safer and age-appropriate online environment	Providers of AI-driven systems can contribute to creating a safer and more enjoyable digital environment for children by taking the following actions: Embrace a multidisciplinary approach and engage with civil society, including academia, to assess the potential impacts of their technologies on the diverse rights of potential users, particularly children. Implement safety and privacy as integral parts of the design process when developing products or services intended for children or commonly used by them. Exercise caution and responsibility in handling children's personal data, given that AI systems rely heavily on data. This includes mindful collection, processing, storage, sale, and publication of children's personal information. Prioritize transparency in AI systems, ensuring that users can understand how and why a system arrived at a specific decision or action. This transparency fosters trust and supports auditing, investigations, and recourse mechanisms when harm to children is suspected. Establish functional and legal mechanisms to address grievances if children experience harm through AI systems. These mechanisms should provide timely redress for discriminatory outcomes and involve oversight bodies for appeals and ongoing monitoring of children's safety and protection. Develop strategies for handling sensitive data, such as reports of abuse or harm shared through their products. Platforms and AI systems should minimize data collection from children and empower children with control over the data they generate. Terms of use should be presented in a way that children can understand, enhancing their awareness and autonomy.

4	Educating children, parents and educators about children's safety and their responsible use of ICTs	Providers of AI-driven systems can enhance their efforts by combining technical measures with educational and empowerment initiatives. They should aim to explain the functionality and objectives of AI systems to child users and their parents or caregivers, enabling them to make informed decisions regarding the use of such platforms.
5	Promote digital technology as a mode to further civic engagement	Providers of AI-driven systems can promote and empower children and young people by upholding their right to participate, as outlined in the general guidelines presented in Table 1.
6	Using technology advances to protect and educate children	AI-driven systems should prioritize children's development and well-being throughout their design, development, and implementation processes. These systems should use established and widely accepted metrics related to development and well-being as their primary benchmarks. Companies should allocate resources for research and development aimed at creating ethical AI tools capable of identifying instances of online child sexual abuse and exploitation (CSAE), as well as online harassment and bullying. Collaboration with experts in children's rights and the direct involvement of children in these efforts is essential. Furthermore, advancements in AI technology should be harnessed to deliver age-appropriate content and messaging to children while safeguarding their identity, location, and personal information.

CONCLUSION

In the rapidly evolving digital landscape, ensuring the safety and well-being of children and young people online is of paramount importance. The COP guidelines outlined in the previous sections provide a comprehensive framework for companies utilizing artificial intelligence (AI)-driven systems to fulfill their responsibilities in protecting children's rights and promoting secure online experiences.

These guidelines underscore the significance of integrating child rights considerations into corporate policies and management processes. AI systems must be designed with a commitment to uphold the rights outlined in the CRC, recognizing the increasing importance of digital experiences in children's lives. An inclusive design approach, taking into account diversity and stakeholder input, is essential for creating inclusive and child-centered AI technologies.

Collaboration with government entities, law enforcement agencies, civil society organizations, and hotline initiatives is crucial for combating child sexual abuse material (CSAM). Standard procedures, proactive cooperation with internal departments, and explicit policies to prohibit illegal content and behaviors are vital aspects of this fight against CSAM.

Creating a safer online environment for children involves multifaceted approaches, including a multidisciplinary evaluation of technology impacts, proactive safety and privacy measures, and mechanisms for addressing grievances. Empowering children with control over their data and ensuring transparency are key to fostering trust and security.

Education initiatives that help children, parents, and educators understand AI systems' functionality and objectives are essential. These initiatives enable informed decisions about platform usage and contribute to safer digital experiences. Moreover, promoting digital technology as a means of fostering civic engagement aligns with children's rights to participate actively in society.

Advancements in AI technology provide opportunities to protect and educate children effectively. Ethical AI tools capable of identifying online threats and harassment, developed through collaboration with children's rights experts and children themselves, hold the potential to enhance online safety. Leveraging AI to deliver age-appropriate content while safeguarding children's identity and personal information is another crucial aspect of promoting child online protection.

In conclusion, the COP guidelines offer a comprehensive roadmap for AI-driven system providers to prioritize child online protection, uphold their rights, and contribute to the creation of a safer and more inclusive digital environment for all. In this age of AI, where digital experiences are integral to children's lives, safeguarding their well-being is a shared responsibility that requires diligence, collaboration, and a steadfast commitment to children's rights.

ACKNOWLEDGEMENTS

These guidelines have been adapted from the ITU's Guidelines for Industry on Child Online Protection 2020 with the majority of the recommendations remaining unchanged. The addition is the inclusion of the unique Bhutanese context. As an effort to localize the guidelines to Bhutanese context and to align them with the specific needs and challenges faced by the Bhutanese community in addressing child online protection, valuable insights gleaned from various relevant reports and Focused Group Discussions (FGDs) conducted with the Industry players in Bhutan.

The GovTech Agency is deeply indebted to the International Telecommunication Union (ITU) for its unwavering guidance and steadfast support in adapting these guidelines to the Bhutanese context. The localized COP guidelines would not have materialized without the ITU's generous financial and technical assistance, and the expertise of its dedicated team. Furthermore, the agency expresses its profound gratitude to UNICEF, Bhutan, a valued ITU partner, for its invaluable contributions throughout the development process.

In addition, the GovTech Agency acknowledges the support and efforts of the Child Online Protection Working Group consisting of the following agencies:

1. Women and Children Division, National Commision for Women and Children
2. Crime Division, Royal Bhutan Police
3. Career Education and Counselling Division, Department of Education Programs, Ministry of Education and Skills Development
4. Bhutan Information Communications & Media Authority
5. Office of the Attorney General
6. BtCIRT, Cybersecurity Division, GovTech Agency
7. Nazoen Lamtoen
8. RENEW (Respect, Educate, Nurture, Empower Women)
9. Department of School Education (DSE), Ministry of Education and Skills Development
10. Bhutan Telecom Ltd.
11. Tashi Cell
12. The former Ministry of Information & Communications
13. The former Department of Information and Media

DISCLAIMER

Australian Government

Department of Infrastructure, Transport, Regional Development, Communications and the Arts

This localization was funded by The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), from the Australian Government. This localization was not created by the International Telecommunication Union (ITU) and should not be considered an official ITU localization. The ITU shall not be liable for any content or error in this localization.

These localized guidelines are based on the ITU's Guidelines for Industry on Child Online Protection 2020 and have been adapted to reflect the unique context and needs of Bhutan. While the ITU guidelines remain the authoritative source of information, these localized guidelines provide additional guidance specific to Bhutan, incorporating insights from various relevant reports and Focused Group Discussions (FGDs) conducted with important Industry players in Bhutan. The localized guidelines were developed with the support from the International Telecommunication Union (ITU).