GUIDELINES FOR POLICY-MAKERS ON CHILD ONLINE PROTECTION (LOCALIZED FOR BHUTAN)

VERSION 1.0
2023

GUIDELINES FOR POLICY-MAKERS
ON
CHILD ONLINE PROTECTION
(LOCALIZED FOR BHUTAN)

VERSION 1.0

2023

TABLE OF CONTENT

ABSTRACT

In an increasingly digital world, the protection of children online has become an urgent concern. To address this, policy-makers must establish a comprehensive national strategy for child online protection. One of the first steps involves a thorough examination of the current legal framework. The law must explicitly extend its authority to empower law enforcement and relevant agencies to safeguard individuals under 18 across all online platforms. It's crucial to acknowledge that any crime against a child that exists in the physical world can also occur in the online sphere, with necessary adaptations. Additionally, regulations concerning online data protection and privacy for children require attention, including the prohibition of specific online behaviors unique to the internet.

The regulatory framework poses another critical consideration. Policy-makers must decide whether to adopt self-regulation, co-regulation, or comprehensive regulation. Self and co-regulation models involve the creation and publication of best practices or safety standards, offering flexibility and agility in response to technological advancements. In contrast, a regulatory model establishes clear expectations and responsibilities within a legal framework, potentially accompanied by penalties for violations. Striking a balance between these approaches is essential.

Reporting mechanisms for illegal online content must be user-friendly and widely publicized. Establishing a national hotline or reporting portal can facilitate the swift removal of illicit materials. Industry entities must proactively detect and eliminate child exploitation instances and offer mechanisms for users to report concerns or issues they encounter within their services.

Engaging all relevant stakeholders is paramount. This includes government agencies, law enforcement, social services organizations, internet service providers, educators, parents, and children themselves. Collaborative efforts can lead to a unified national initiative aimed at enhancing online safety for children. Research can provide insights into the level of responsibility and existing initiatives of these entities.

Education plays a crucial role in equipping children with digital literacy skills. Integrating age-appropriate digital literacy components into the national educational curriculum can empower students to navigate the online world safely. It's essential to emphasize the positive aspects of technology while fostering responsible online behavior. Educators must receive training to effectively teach these skills and recognize signs of abuse.

To establish comprehensive child protection, standardized procedures should require all professionals and institutions involved with children to recognize, address, and report instances of online abuse and harm. Nationwide awareness campaigns can amplify the importance of online child protection on a universal scale, involving parents, guardians, and educators. Finally, evaluating device configurations and promoting user accountability through security software and settings are essential components of a national child online protection strategy.

DOCUMENT OVERVIEW

Purpose

The Royal Government of Bhutan has a duty to ensure the safety of children in both the physical and digital realms. In today's world, where technology is deeply integrated into the lives of young people, maintaining a strict division between offline and online experiences is no longer feasible. These two aspects are increasingly interconnected and reliant on each other.

Policy-makers[1] and other relevant stakeholders play crucial roles in this regard. The rapid pace of technological advancement means that traditional policymaking methods are no longer adequate. Policy-makers must create a legal framework that is adaptable, inclusive, and suited for the rapidly changing digital landscape to safeguard children online.

The purpose of these guidelines is to provide policy-makers with a user-friendly and flexible framework to understand and fulfill their legal responsibility to protect children in both the physical and virtual worlds. To achieve this, the guidelines address several key questions for policy-makers:

1. What does child online protection entail?
2. Why is it important for policy-makers to prioritize child online protection?
3. What is the legal, socio-political, and developmental context of their country?
4. How should policy-makers go about developing an effective and sustainable child online protection policy in their nation?

In doing so, these guidelines utilize existing models, frameworks, and resources to provide context and offer insights into best practices from around the world.

Scope

Child online protection encompasses a wide range of risks that can harm children in digital spaces. This is a complex issue that requires a multifaceted approach involving laws, governance, education, policies, and societal efforts.

Furthermore, child online protection should be based on an understanding of both general and country-specific risks, threats, and harms that children face online. This involves clear definitions and guidelines that distinguish between actions that constitute a crime and those that, while not illegal, still pose a threat to a child's well-being.

The guidelines aim to provide an overview of the current digital threats and harms faced by children. However, the rapid evolution of technology and associated risks means that traditional policymaking methods are insufficient. Policy-makers in the digital age must create legal and policy frameworks that are adaptable and inclusive, capable of addressing existing challenges and anticipating future ones. Achieving this requires collaboration with various stakeholders, including the information and

[1] The term policy-makers refers here to all stakeholders that are responsible for developing and implementing policy, particularly those within government

Communication Technology (ICT) industry, research community, civil society, the public, and even children themselves. Establishing overarching principles for child online protection can support this process.

Overarching principles

The following eleven principles, presented here, collectively serve as a framework for the development of a comprehensive national strategy for the protection of children in the online environment. It is important to note that the order in which these principles are listed is based on a logical progression of ideas rather than any indication of their relative importance.

A national strategy for child online protection should:

1. Be founded upon a holistic vision that encompasses the participation of government, industry, and society.
2. Emerge from a comprehensive understanding and assessment of the overall digital landscape, while remaining adaptable to the specific circumstances and priorities of the country.
3. Uphold and align with the fundamental rights of children, as established in international agreements like the UN Convention on the Rights of the Child and other pertinent international laws and conventions.
4. Respect and remain in harmony with existing domestic legislation and strategies related to child protection, including laws concerning child abuse or child safety.
5. Safeguard the civil rights and freedoms of children, ensuring that protection efforts do not compromise these fundamental rights.
6. Be collaboratively developed with the active engagement of all relevant stakeholders, including children themselves, while addressing their unique needs and responsibilities and considering the interests of minority and marginalized groups.
7. Be strategically designed to align with broader government initiatives for economic and social advancement, harnessing the potential of ICTs to promote sustainable development and social inclusion.
8. Employ the most suitable policy instruments available to achieve its objectives, taking into account the specific circumstances of the country.
9. Be established at the highest levels of government, with a clear allocation of roles and responsibilities, along with the allocation of adequate human and financial resources.
10. Foster the creation of a digital environment that inspires trust among children, parents/caregivers, and stakeholders.
11. Direct the efforts of various stakeholders toward empowering and educating children in digital literacy, equipping them to protect themselves effectively in the online realm.

Usage of these guidelines

These guidelines are informed by pertinent research, established models, and available resources, offering clear recommendations for the formulation of a comprehensive national strategy aimed at safeguarding children in the digital world.

- Section 2 provides an introduction to the concept of child online protection and offers insights drawn from recent research. This includes considerations of emerging technologies and an exploration of the primary threats and risks confronting children in the online environment.
- Section 3 delineates the preparatory steps necessary for the development of a national child online protection strategy. It encompasses the identification of relevant stakeholders, references exemplary responses to online threats and harms, and underscores the advantages of having a well-defined national strategy.
- Section 4 offers recommendations pertaining to frameworks and the practical execution of the strategy.
- Section 5 presents a series of national checklists designed to facilitate the creation of a national child online protection strategy.
- Section 6 provides a valuable compendium of reference materials for further guidance and information.

INTRODUCTION

In 2019, more than half of the global population utilized the Internet, with the largest user demographic being those under 44 years old. Usage was particularly high among 16 to 24-year-olds and 35 to 44-year-olds. Globally, one in three children, aged 0-18[2], accessed the Internet, and this number is expected to more than double over the next five years[3], especially in developing countries. New generations are growing up with the Internet, predominantly through mobile network technology, particularly in the global south[4].

In Bhutan, in 2020, about 68 percent of students reported using the Internet. Among them, 34 percent spent 1 to 2 hours on digital devices daily, while 30 percent used them for less than an hour. A smaller group, constituting four percent, spent seven hours or more online. This trend can be attributed to the widespread availability of Internet access points, the prevalence of mobile technology, and the increasing variety of Internet-enabled devices. These factors, combined with the vast resources available online, present unprecedented opportunities for learning, sharing, and communication[5].

However, while Internet access is crucial for children's rights, disparities in access still exist based on region, nationality, gender, and other factors, limiting opportunities for girls, children with disabilities, and other vulnerable groups. In terms of the digital gender divide, research shows that, except in the United States of America, male Internet users significantly outnumber female users in most regions. Girls in many countries face not only restricted Internet access but also monitoring and safety risks when trying to connect online[6]. It's evident that children and young people lacking digital skills or speaking minority languages may struggle to find relevant online content, while rural children may have fewer digital skills, spend more time online (especially playing games), and receive less parental guidance and supervision[7].

Despite these challenges, it's important to acknowledge the enriching and empowering nature of digital technology. The Internet and digital technologies have transformed the way we live, offering new avenues for communication, entertainment, education, and skill development. The Internet also provides crucial access to health and educational services, as well as information on topics that may be otherwise taboo in certain societies.

Children and young people are at the forefront of embracing and adapting to the opportunities presented by the Internet. However, they are also exposed to various online risks and welfare-related issues that require open discussion. Such discussions create a platform for teaching children and young people how to recognize and mitigate risks and harms while harnessing the advantages and opportunities offered by the Internet.

[2] OECD, "New Technologies and 21st Century Children: Recent Trends and Outcomes," OECD Education Working Paper No. 179 (Directorate for Education and Skills, OECD), accessed January 27, 2020, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282018%2915&docLanguage=En.

[3] Ofcom, "Children and Parents: Media Use and Attitudes Report 2018" (Ofcom), accessed January 17, 2020, https://www.ofcom.org.uk/%20data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf.

[4] ITU, "Measuring the Information Society Report," accessed January 16, 2020, https://www.itu.int/dms_pub/%20itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf.

[5] MOIC, (2021), National ICT Household Survey, Nationwide ICT Household Survey Report. https://www.gage.odi.org/publication/digital-media-risks-opportunities/

[6] Young Adolescents and Digital Media: Uses, Risks and Opportunities in Low-and Middle-Income Countries,"GAGE, accessed January 29, 2020,

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

Many young people around the world possess a good understanding of some of the risks they face online[8]. For instance, research shows that most children and young people can distinguish between cyberbullying and online teasing. However, striking a balance between a child's online opportunities and risks remains a challenge[9].

For ITU Member States, safeguarding children and young people online is a priority, but it must be balanced with efforts to promote online opportunities for them[10]. These efforts should protect children and young people without impeding their access or the broader public's access to information, freedom of speech, expression, and association.

There is an evident need for dedicated investments and innovative solutions to address the risks faced by children and young people online, particularly due to the digital divide between children and adults, limiting guidance from parents, teachers, and guardians. As children grow into adults, parents and active members of society, there is an opportunity to reduce this digital divide.

In this context, building trust in the Internet should be a central focus of public policy. Governments and society should collaborate with children and young people to understand their perspectives and facilitate genuine public discussions about online risks and opportunities. While supporting children and young people in managing online risks is essential, governments should also ensure the availability of support services for those who experience harm online and educate children on how to access these services.

While some countries may face challenges in allocating sufficient resources for digital literacy and online safety, children report that parents, teachers, technology companies, and governments play crucial roles in developing solutions to support their online safety. International Telecommunication Union (ITU) Member States have expressed significant support for enhanced knowledge sharing and coordinated efforts to enhance online safety for a greater number of children.

Children and young people are navigating an increasingly complex digital landscape, and the integration of artificial intelligence, machine learning, big data analytics, robotics, virtual and augmented reality, and the Internet of Things is poised to transform their media practices. Policymaking and investments are needed not only for the current generation but also to prepare for the digital future of children, parents, and communities.

[8] ITU, Youth Consultation, https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx.
[9] UNICEF, "Global Kids Online Comparative Report (2019)."
[10] ITU, "Celebrating 10 Years of Child Online Protection", ITU News, February 6, 2018, https://news.itu.int/%20celebrating-10-years-child-online-protection/

WHAT IS CHILD ONLINE PROTECTION?

Online technologies provide children and young people with numerous opportunities to communicate, acquire new skills, express creativity, and contribute positively to society. However, these technologies also introduce new risks, such as privacy breaches, exposure to illegal content, harassment, cyberbullying, misuse of personal data, grooming for sexual purposes, and even child sexual abuse.

These guidelines establish a comprehensive approach to address all potential threats and harms that children and young people may encounter as they develop digital literacy. They acknowledge that all relevant stakeholders play a role in enhancing digital resilience, well-being, and protection while enabling children and young people to harness the opportunities offered by the Internet.

Protecting children and young people is a collective responsibility, and it falls upon various stakeholders, including policy-makers, industry players, parents, caregivers, educators, and others, to ensure a sustainable future for all. To achieve this, stakeholders must ensure that children and young people can realize their potential both online and offline.

While there is no universally accepted definition of child online protection, the goal is to adopt a comprehensive approach to create secure, age-appropriate, inclusive, and participatory digital environments for children and young people. These environments should encompass:

- The ability to respond, seek support, and help themselves when facing online threats.
- Measures for the prevention of harm.
- A dynamic equilibrium that ensures protection while allowing children to be active digital citizens.
- The upholding of rights and responsibilities for both children and society.

Moreover, owing to the rapid evolution of technology and society and the global nature of the Internet, child online protection must be flexible and adaptable to remain effective. While these guidelines provide insights into the primary risks faced by children and young people online, such as harmful content, harassment, cyberbullying, data misuse, grooming for sexual purposes, child sexual abuse, and exploitation, new challenges will inevitably emerge with technological advancements. These challenges may vary by region. However, addressing new challenges is best achieved through global collaboration, as innovative solutions need to be developed collectively within the global community.

CHILDREN IN THE DIGITAL WORLD

The Internet has brought about a profound transformation in our way of life, becoming an integral part of the daily existence of children and young people. It is no longer feasible to separate the digital and physical realms, as they are deeply intertwined. Presently, one-third of all Internet users are individuals under the age of 18, and UNICEF estimates that 71 percent of young people are already active online[11].

This connectivity has had a significantly empowering effect. The online world has provided children and young people with opportunities to surmount disadvantages and disabilities. It has also created new arenas for entertainment, education, engagement, and relationship-building. Digital platforms serve as versatile tools for a wide range of activities, often offering multimedia experiences.

[11] ITU, 2020, Guidelines for Policy-makers on Child Online Protection, https://www.itu-cop-guidelines.com/

Accessing and learning to use and navigate this technology is deemed crucial for the development of young people, and they often begin using digital platforms and services at an early age, even before they reach the prescribed minimum age. Therefore, it is essential for policy-makers to recognize that education in this context should commence early.

Children and young people are eager to participate in discussions concerning the online environment, possessing valuable expertise as "digital natives" that can be shared. Policy-makers and practitioners must engage in ongoing dialogues with children and young people to support their rights in the digital realm.

Access of Internet: In Bhutan, approximately 60 percent of households have children below the age of 15 years. Among these households, slightly over half, specifically 54.1 percent, report that their children have access to the Internet. Notably, urban households exhibit a higher proportion of children with Internet access, accounting for 65.8 percent, compared to their rural counterparts, where this figure stands at 46.7 percent.

Among the households granting Internet access to children (representing 54 percent of households), the majority of children, comprising 65.2 percent, prefer to access the Internet using their parents' mobile phones. Additionally, for children who possess their own mobile phones, a significant portion, accounting for 43.6 percent, prefer to access the Internet through their personal devices.

Mobile phones emerge as the favored ICT equipment among children for Internet access. However, it is noteworthy that internet cafes are not a preferred choice, with only a negligible percentage, specifically 0.08 percent, of children selecting this option. Similarly, children do not favor using their schools' resources for Internet access, with only 0.5 percent opting for this method.

Concerning daily Internet usage patterns, 66.3 percent of children typically spend one to three hours per day online, while in 28.6 percent of households, children's daily Internet usage is less than one hour. Interestingly, the frequency of Internet use appears to be fairly consistent between rural and urban children. However, it is worth noting that Punakha has the highest percentage of children, accounting for 81 percent, who spend more than one hour but less than three hours online each day, while Trashi Yangtse has the lowest proportion, representing 39.6 percent, of children with this level of Internet use[12].

Use of the Internet: Online gaming holds the highest appeal among Bhutanese children, with approximately 80 percent showing a preference for downloading and playing games over the internet. This preference remains consistent among both rural and urban children. Moreover, a significant majority of children, specifically 73.4 percent, derive enjoyment from viewing or downloading photos, videos, and music from the internet. At least 19.2 percent of children engage in various online activities, such as chatting, blogging, reading news, and participating in online discussions. Some children actively participate in social media networks and contribute self-generated content online, although the exact proportion remains unspecified. Furthermore, a small but noteworthy fraction, 1.6 percent, have ventured into online shopping or the procurement of goods and services via the internet, indicating an emerging interest in e-commerce within the Bhutanese child demographic[13].

[12] MOIC, (2021), National ICT Household Survey, Nationwide ICT Household Survey Report.
[13] MOIC, (2021), National ICT Household Survey, Nationwide ICT Household Survey Report.

THE IMPACT OF TECHNOLOGY ON CHILDREN'S DIGITAL EXPERIENCE

The Internet and digital technology offer both opportunities and risks to children and young people. For instance, when children use social media, they can benefit from numerous opportunities for exploration, learning, communication, and skill development. Social networks, in particular, are viewed by children as safe platforms to explore personal identity. Possessing relevant digital skills and knowledge to address privacy and reputation-related issues is crucial for young people.

However, consultations have indicated that most children use social media platforms before the minimum age of thirteen[14], and age verification services are generally inadequate or nonexistent, which can intensify the risks they face. While children are eager to acquire digital skills and become responsible digital citizens, they often think about privacy concerning their friends and acquaintances, rather than strangers and third parties. This, combined with children's natural curiosity and relatively lower risk threshold, can make them vulnerable to grooming, exploitation, bullying, or exposure to harmful content or contact.

Student participants in the focus group discussions (FGDs) do not possess direct knowledge of school friends or acquaintances who had encountered online hate speech and violence. Consequently, they were unable to provide specific details on how such situations were managed or any resulting behavioral changes. Nonetheless, these students emphasized the importance of reporting incidents of online violence and seeking support. They stressed the need to report such challenges to parents, school authorities, or the police, underscoring the significance of having a support network comprising friends, peers, or adults to cope with these difficulties.

The widespread popularity of image and video sharing through mobile apps, especially the use of live streaming platforms by children, raises additional privacy and risk concerns. Some children produce and share sexual images of themselves, friends, or siblings online. For older children, this may be viewed as a natural exploration of sexuality and sexual identity, while younger children may experience coercion by an adult or another child. Regardless of the circumstances, the resulting content is illegal in many countries and can expose children to the risk of legal action or further exploitation.

Similarly, online gaming allows children to exercise their fundamental right to play, build networks, spend time with new friends, and develop essential skills. In most cases, this has a positive impact. However, there is growing evidence that unmonitored and unsupported use of online gaming platforms by children can lead to risks such as gaming disorders, financial dangers, the collection and monetization of children's personal data, cyberbullying, hate speech, violence, and exposure to inappropriate behavior or content[15]. Additionally, there is the risk of grooming, involving real, computer-generated, or virtual reality images and videos depicting and normalizing the sexual abuse and exploitation of children.

Furthermore, advancements in technology have given rise to the Internet of Things (IoT), where an expanding array of devices can connect, communicate, and network over the Internet. This encompasses toys, baby monitors, and artificial intelligence-powered devices, which may pose privacy and unwanted contact-related risks.

[14] Contectados al Sur network, "Hablatam"; UNICEF, "Global Kids Online Comparative Report (2019)."
[15] UNICEF, "Global Kids Online Comparative Report (2019)." (UNICEF, 2019)

KEY THREATS TO CHILDREN ONLINE

Both adults and children encounter various risks and threats in the online environment. However, it is vital to recognize that children constitute a more vulnerable segment of the population, with certain groups of children, such as those with disabilities or children on the move[16], being even more susceptible to these risks. Policy-makers must ensure that all children have the opportunity to grow and receive education in a secure digital environment. This concept of safeguarding children from all forms of exploitation due to their vulnerability is enshrined in the UN Convention on the Rights of the Child.

Within the digital realm, several aspects offer substantial opportunities for children but can also magnify risks that have the potential to profoundly harm them and compromise their well-being. Concerns exist, shared by both adults and children, regarding the Internet's potential for invading personal privacy, propagating misinformation, or, worse, facilitating access to explicit content. Table 1 shows the classification of online risks to children.

Table 1: Classification of online risks to children

	Content Child as receiver (of mass productions)	**Contact** Children as participant (adult-initiated activity)	**Conduct** Child as actor (perpetrator/victim)
Aggressive	Violent/gory content	Harassment, stalking	Bullying, hostile peer activity
Sexual	Pornographic content	'Grooming', sexual abuse on meeting strangers	Sexual harassment, 'sexting'
Values	Racist/hateful content	Ideological persuasion	Potentially harmful user-generated content
Commercial	Advertising, embedded marketing	Personal data and exploitation and misuse	Gambling copyright infringement

Source: EU Kids Online (Livingstone, Haddon, GÖrzig, and Olafsson, 2010)[17]

It is essential to distinguish between risks and actual harm when it comes to children. Not every activity carrying an element of risk is inherently dangerous, and not all risks inevitably result in harm to children. For instance, sexting, which represents a way young people might explore their sexuality and relationships, does not necessarily entail harm.

The onset of the digital era has introduced new complexities in child protection. It is imperative that children are empowered to safely navigate the online environment and harness its numerous benefits. To achieve this, policy-makers must ensure the existence of pertinent legislation, safeguards, and tools that facilitate a secure environment for children's development and learning. Equally crucial is equipping children with the requisite skills to recognize threats and gain a comprehensive understanding of the implications and nuances of their online behavior.

[16] Lundy et al., "TWO CLICKS FORWARD AND ONE CLICK BACK," Report on children with disabilities in the digital environment (Council of Europe, October 2019), https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.
[17] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full findings. LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/

Content and manipulation

During their online interactions, children can encounter a multitude of threats originating from organizations, adults, and their peers. These threats encompass the following aspects:

1. **Content and Manipulation:** Exposure to inappropriate or even illegal content can potentially lead children to extreme behaviors such as self-harm, destructiveness, or violence. Furthermore, exposure to such content can also result in radicalization or the adoption of racist or discriminatory ideologies. It is recognized that many children do not adhere to age restrictions imposed on websites.

2. **Dissemination of Inaccurate or Incomplete Information:** Exposure to information that is inaccurate or lacking in completeness can hinder children's understanding of the world around them. The practice of tailoring content based on user behavior can result in the formation of "filter bubbles," which restrict children's access to diverse content.

3. **Algorithmically Filtered Content for Manipulation:** Exposure to content that is algorithmically manipulated with the intent to influence can significantly shape a child's development, opinions, values, and habits. Isolating children within "echo chambers" or "filter bubbles" prevents them from accessing a wide spectrum of opinions and ideas.

Contact from adults or peers

Children may confront a diverse array of contact-related threats originating from their peers or adults in the online sphere. These threats encompass the following:

1. **Online Bullying:** Online bullying can propagate rapidly and extensively, surpassing the speed and reach of offline bullying. It can transpire at any hour, thereby intruding upon previously regarded "safe spaces," and often it can be conducted anonymously.

2. **Higher Risk for Children with Disabilities:** Children who are victims of offline victimization are predisposed to experiencing online victimization as well. This heightened risk is particularly pronounced for children with disabilities, as research indicates that they are more susceptible to various forms of abuse, including sexual victimization. Such victimization encompasses bullying, harassment, exclusion, and discrimination, often rooted in a child's actual or perceived disability or related factors, such as their behavior, speech, or use of specialized equipment or services.

3. **Defamation and Damage to Reputation:** Images and videos can be manipulated and disseminated to a vast global audience. Injudicious comments or actions can endure for extended periods, remaining accessible for anyone to view.

4. **Online Targeting and Grooming:** Children can be targeted, groomed, and subjected to abuse by online offenders, whether locally or from distant parts of the world. These perpetrators often adopt false identities, claiming to be someone they are not. Such forms of victimization can encompass radicalization or coercing children into sharing sexually explicit content of themselves.

5. **Financial Exploitation:** Children may face pressures, deception, or coercion, leading them to make purchases, with or without the permission of the bill payer.

6. **Unwanted Advertising:** The proliferation of unwanted advertising raises concerns related to consent and the commodification of children's data.

Conduct of the child, potentially leading to consequences

Online bullying can have profoundly distressing and injurious consequences due to various factors:

1. **Wider Dissemination:** Online bullying can spread extensively and garner greater visibility, making it challenging for victims to find closure as the electronically circulated content can resurface at any time.

2. **Harmful Content:** Bullying in digital spaces may involve damaging visual images or hurtful words, intensifying the emotional impact on victims.

3. **Persistent Availability:** Online bullying is accessible 24 hours a day, intruding into a victim's privacy even within ostensibly safe environments, such as their home.

4. **Manipulation of Personal Information:** Perpetrators can manipulate personal information and alter visual images, subsequently disseminating them to others, exacerbating the harm.

5. **Anonymity:** Online bullying can be conducted anonymously, shielding the identity of the aggressor. Disclosure of personal information increases the risk of physical harm, potentially leading to real-life encounters with online acquaintances, which may culminate in physical and/or sexual abuse.

Other concerning online behaviors involve:

1. **Infringement of Rights:** Children may infringe upon their own rights or the rights of others through activities such as plagiarism or uploading content without permission. This may include the unauthorized capture and sharing of inappropriate photos.

2. **Copyright Infringement:** Infringement of copyright, such as downloading music, films, or TV programs without proper authorization, can be detrimental, both ethically and legally.

3. **Compulsive Internet Use:** Compulsive and excessive use of the Internet or online gaming, to the detriment of social and outdoor activities essential for health, confidence building, social development, and overall well-being.

4. **Harming Others:** Some individuals may attempt to harm, harass, or bully someone else, often by assuming a false identity, which is a common tactic among children.

5. **Sexting:** An increasingly common behavior among teenagers involves "sexting," which entails sharing sexualized images or text via mobile phones. While these exchanges may initially occur within relationships or with potential partners, they can inadvertently reach much broader audiences. Young teenagers may not fully grasp the implications and potential risks associated with these behaviors.

Key harms for children online

The preceding section discussed the various threats that children may encounter in the online environment. This section will now emphasize the specific harms that can result from these threats.

Harms

UNICEF studies on Internet use identify the following categories as risks and harms:

- **Self-Abuse and Self-Harm:** This category encompasses content related to suicide and discrimination.
- **Exposure to Unsuitable Materials:** It includes exposure to extremist, violent, gory content, embedded marketing, and online gambling.

Approximately 20 percent of children surveyed reported encountering websites or online discussions about self-harm or physical harm to individuals in the past year.

- **Radicalization:** This involves ideological persuasion and hate speech.

Children were more likely to report being upset by hate speech or sexual content online, being treated in a hurtful way online or offline, or by meeting someone in person whom they had initially encountered online.

- **Sexual Abuse and Exploitation:** This category encompasses self-generated content, sexual grooming, child sexual abuse material (CSAM), trafficking, and sexual exploitation of children in travel and tourism.

A 2017 study in Denmark, Hungary, and the United Kingdom found that 6 percent of children had explicit pictures of themselves shared without their consent.

In 2019, the Internet Watch Foundation (IWF) identified over 132,000 webpages confirmed to contain images and videos of child sexual abuse. Each webpage could contain varying numbers, ranging from one to thousands, of such abusive images[18].

The risks associated with online violence, including the unauthorized sharing of explicit photos and sexual cyberbullying, are characterized by pronounced gender disparities. Girls tend to bear a greater burden of gender-related pressures toward engaging in sexual behavior, resulting in more adverse consequences and harm.

1. **Violation and Misuse of Personal Data:** This category encompasses activities such as hacking, fraud, and theft. While scams and hacking are commonly known, intrusions into a child's online activities are viewed as an additional form of violation. Adults often engage in surveillance of young individuals' mobile phones and online activities. Reports from children in Brazil, for instance, indicate that both boys and girls, spanning various age groups, perceive parents as exerting more control over girls' internet use. This may be attributed, in part, to the

[18] Livingstone, S., Mascheroni, G., Ólafsson, K., and Haddon, L., (2014) Children's online risks and opportunities: comparative findings from EU Kids Online and Net Children Go Mobile. London: London School of Economics and Polilcal Science, https://www.eukidsonline.net/ and http://www.netchildrengomobile.eu/.

societal structures in which girls live, particularly concerning their safety, within an environment where the line between online and offline interactions becomes increasingly blurred.

2. **Cyberbullying, Stalking, and Harassment:** This pertains to hostile and aggressive peer behavior. Chat rooms and social networking platforms can serve as venues for violence and bullying, with anonymous users, including young individuals, engaging in aggressive or abusive communication. In a study spanning seven European countries, cyberbullying affected 8 percent of children on average in 2010, rising to 12 percent in 2014. While data specific to Bhutan is unavailable, participants in focus group discussions highlighted incidents of cyberbullying, where children face harassment, threats, and humiliation. However, awareness of cyberbullying remains limited, with only approximately 13 percent of households being aware of their children's exposure to such incidents. It is crucial to note that vulnerable children are often at a heightened risk of becoming victims of cyberbullying[19].

In focus: Enhancing inequalities

In 2017, around 60 percent of children in the Africa region did not have access to the internet, in stark contrast to Europe, where only 4 percent of children were offline. Across all world regions, male internet users outnumbered female users, and internet usage by girls was frequently subject to monitoring and restrictions. The expansion of broadband connectivity to previously unconnected regions of the world is expected to exacerbate this inequality[20].

In Bhutan, among 15-year-old students, only 6.7 percent were not connected to the internet, with a higher proportion of girls (8.2 percent) lacking access compared to boys (4.8 percent)[21].

Research indicates that a substantial portion (15 percent) of individuals in Bhutan face considerable obstacles in their online engagement. For many, these challenges primarily revolve around access issues, including inadequate connectivity, the high costs associated with data and devices, and a scarcity of suitable equipment (footnote 20).

As affordable broadband services expand into developing regions, it becomes increasingly imperative to implement measures that can mitigate the risks and threats faced by these children while simultaneously enabling them to leverage the full spectrum of advantages offered by the digital realm.

In Focus: Child Sexual Abuse Material (CSAM)

1. The scale of the problem

The Internet has revolutionized the scale and nature of the production, distribution, and availability of child sexual abuse material (CSAM). In 2018, technology companies based in the United States of America reported over 45 million online images and videos suspected of depicting children being sexually abused from various parts of the world. This represents a global industry, and despite efforts to combat it, the extent and seriousness of the abuse are on the rise.

[19] MOIC, (2021), National ICT Household Survey, Nationwide ICT Household Survey Report.
[20] Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation
[21] MOE, (2020), Digital Kids Asia Pacific, The Country report Bhutan.

In the past, in an offline context, individuals seeking CSAM had to take substantial risks and incur significant expenses to access such material. However, the Internet has made it comparatively easy for offenders to access this content and engage in increasingly risky behaviors. The prevalence of small, integrated cameras in our daily lives has made the production of CSAM and the acquisition of content from non-contact abuse more accessible than ever before.

It is impossible to precisely quantify the size or structure of this clandestine and illegal enterprise. Nevertheless, it is evident that the number of illegal images currently in circulation is in the millions. Nearly all the children featured in these images have had their images duplicated. In 2018, the Internet Watch Foundation (IWF) monitored how frequently images of a child who had been rescued in 2013 resurfaced. Over a span of three months, IWF analysts observed these images appearing 347 times, equivalent to five times each working day.

2. The current landscape

Whenever an image of a child being abused appears and circulates online, or when it is downloaded by an offender, that child is subjected to re-abuse. Victims are forced to live with the enduring presence and circulation of these images for the rest of their lives.

When material depicting child sexual abuse or a webpage hosting such content is identified, it is crucial to promptly remove or block the content. However, due to the global reach of the Internet, this can be challenging, as offenders can create content in one country, host it in another, and target consumers in a third country. The execution of national warrants or notices often requires intricate international cooperation, making it a complex task.

The rapid pace of technological advancements in the digital realm means that the landscape of offenders is constantly evolving. Notable emerging threats include:

- The proliferation of encryption unintentionally provides offenders with hidden channels to operate and share illegal material, making detection and law enforcement more difficult.
- Forums dedicated to the grooming of children are growing in concealed corners of the Internet, normalizing and encouraging such behavior, often demanding 'new content' for entry.
- The swift expansion of Internet access is enabling users to go online in regions that have yet to establish comprehensive safety measures or the necessary infrastructure.
- Children are increasingly using digital devices at younger ages without supervision, and sexual behavior online is becoming more normalized. The number of self-generated images of abuse is increasing each year[22].

In Focus: Self-generated content

Children and adolescents may engage in the practice of capturing compromising images or videos of themselves. While this behavior is not necessarily unlawful and may occur as a part of normal and healthy sexual development, there are inherent risks associated with any such content being disseminated online or offline, potentially causing harm to children or serving as a means for extortion.

[22] ITU, 2020, Guidelines for Policy-makers on Child Online Protection, https://www.itu-cop-guidelines.com/

It is important to note that while some children may feel pressured or coerced into sharing explicit images, others, particularly adolescents, may willingly create such content. However, this willingness should not be construed as consent to or responsibility for the exploitative or abusive use and distribution of these images.

Sexting, which encompasses the self-production of sexual images or the exchange of sexual messages or images[23], involves creating, sharing, and forwarding sexually suggestive nude or nearly nude content through mobile phones and/or the Internet. This practice of sexting is diverse in terms of context, meaning, and intention[24].

While sexting is perhaps the most common form of self-generated sexually explicit content involving children, often occurring among consenting adolescents who find pleasure in the activity, there are instances of unwanted sexting as well. Unwanted sexting refers to non-consensual aspects of the activity, such as the sharing or receiving of sexually explicit photos, videos, or messages without consent, potentially by individuals known or unknown to the child who are attempting to make contact, exert pressure, or groom the child. Sexting can also manifest as a form of sexual bullying, where a child is coerced into sending an image to a boyfriend, girlfriend, or peer who then disseminates it within their peer network without the child's consent.

In Focus: Cyberbullying

Bullying, as a phenomenon, has existed long before the Internet came into being. However, the Internet has introduced new elements that can magnify the scale, reach, and persistence of bullying, thereby exacerbating an already distressing and harmful experience for its victims. Cyberbullying is characterized by deliberate and repetitive harm inflicted on individuals through the use of computers, mobile phones, and other electronic devices. It often occurs concurrently with offline bullying incidents, whether at school or elsewhere. Cyberbullying can exhibit additional dimensions related to racism, religion, or sexism, and it may serve as an extension of harm experienced offline. This extension can manifest through actions such as hacking into accounts, sharing photos and videos online, and the continuous nature of hurtful messages, as well as the availability of harmful content 24/7. Cyberbullying is typically considered a social issue rather than a criminal one. Addressing cyberbullying necessitates a comprehensive approach that involves collaboration among schools, families, and, critically, children themselves.

In Focus: Online grooming and sextortion

Due to rapid technological advancements and increased Internet and digital communication access, there has been a heightened risk of online criminal activities targeting children. Among these emerging forms of online child sexual exploitation, two significant concerns are online grooming and sextortion. Online grooming broadly encompasses the process where an adult establishes a connection and influences a child (under 18 years old) through the Internet or other digital means with the aim of facilitating contact or non-contact sexual interactions with that child. During grooming, an offender

[23] Karen Cooper et al., "Adolescents and Self-Taken Sexual Images: A Review of the Literature," Computers in Human Behaviour 55 (February 2016): 706–16, https://doi.org/10.1016/j.chb.2015.10.003.
[24] UNODC, "Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children" (Vienna: UN, 2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.

seeks to gain the child's compliance, maintain secrecy, and evade detection and punishment[25]. It is essential to acknowledge that instances of peer-on-peer abuse also exist.

According to INTERPOL, the Internet provides groomers with a vast pool of easily accessible potential targets, enabling them to present themselves in ways that attract children. Online child sex offenders employ manipulation, coercion, and seduction to lower a child's inhibitions and persuade them to engage in sexual activities. Groomers systematically identify vulnerable potential victims, gather intelligence about the child's family support, and use pressure, shame, or fear to sexually exploit a child. Groomers may leverage adult pornography and child abuse materials to desensitize their potential victims, portraying child sexual activity as normal. The Internet has transformed the dynamics of human interaction and redefined the concept of 'friendship.' Establishing an online friendship with a child has become easy and rapid, necessitating a re-evaluation of traditional 'stranger danger' education messages.

Online grooming was officially recognized as an international legal concern in 2007 through the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). Article 23 of the convention criminalizes the "solicitation of children for sexual purposes," requiring an intentional proposal to meet the child for sexual offenses, followed by material acts leading to such a meeting. In many grooming cases, children experience sexual abuse and exploitation online, and the required 'meeting' under the Lanzarote Convention and various national laws is entirely virtual but equally harmful to the child as a physical meeting. Thus, it is crucial to extend the criminalization of grooming to cases when sexual abuse occurs online[26].

Sextortion can occur independently or as a part of online grooming. While sextortion can happen without the grooming process, in some instances, grooming may lead to sextortion[27]. Sextortion may take place within the context of online grooming as groomers manipulate and exert influence over children during grooming, using threats, intimidation, and coercion to obtain sexually explicit images of the child (self-generated content)[28]. If the victim does not comply with the demands for sexual favors, additional intimate images, money, or other benefits, their images may be posted online to cause humiliation or distress or to coerce the child into creating more explicit material. Sextortion has been characterized as "virtual sexual assault" due to its similar emotional and psychological impact on victims. In some cases, the abuse is so traumatic that victims attempt self-harm or suicide to escape it[29].

Europol has noted that collecting data to assess the extent of sextortion affecting children is challenging and likely significantly underreported. Additionally, the absence of common terminology and definitions

[25] International Centre for Missing & Exploited Children, "Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review," 1st Edition (International Centre for Missing & Exploited Children, 2017), https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.
[26] Lanzarote Committee, Committee of the Parties to the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, Solicitation of children for sexual purposes through information and communication technologies (grooming), Opinion on Article 23 of the Lanzarote Convention and its explanatory note, Jun. 17, 2015, https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html
[27] National Center for Missing and Exploited Children (NCMEC), Sextortion, http://www.missingkids.com/%20theissues/onlineexploitation/sextortion.
[28] Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, http://luxembourgguidelines.org/english-version.
29 Benjamin Wittes et al., "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault" (Brookings Institution, May 11, 2016), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.

for online grooming and sextortion hinders the accurate collection of data and a comprehensive understanding of the global scope of these issues[30].

CHILDREN WITH VULNERABILITIES

Children and adolescents can be susceptible to various vulnerabilities, and research conducted in 2019 noted that the digital aspects of vulnerable children's lives often do not receive the same detailed and empathetic consideration as the challenges they face in their offline lives. The report further emphasizes that, in most cases, these children and young people are provided with the same general online safety guidance as their peers, even though they may require specialized support.

While there are numerous specific vulnerabilities that children can experience, including migrant children, those with autism spectrum disorder, and children with disabilities, among others, these three examples are illustrative of the broader range of vulnerabilities children may encounter.

Migrant children

Children and adolescents with migrant backgrounds often bring their unique socio-cultural perspectives and expectations to a new country or to the one they already reside in. While technology is typically viewed as a tool for connection and participation, the online risks and opportunities can vary significantly depending on the context. Moreover, empirical research highlights several critical roles that digital media serve:

- Digital media are essential for orientation, particularly for individuals navigating a new country.
- They play a central role in helping migrants become familiar with the society and culture of the host country.
- Social media platforms can be crucial for maintaining connections with family and peers, as well as accessing important information.

Despite these positive aspects, the use of digital media by migrants can also present challenges, including:

- **Infrastructure:** It is crucial to establish safe online spaces to ensure the privacy and safety of migrant children and young people.
- **Resources:** Migrants often allocate a significant portion of their funds to pre-paid phone cards and digital communication.
- **Integration:** In addition to providing access to technology, it is important to offer effective digital education to support the integration of migrant children and young people into the digital landscape.

[30] Europol, "Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective" (European Cybercrime Centre, May 2017), https://www.europol.europa.eu/sites/default/files/%20documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

Children with Autism Spectrum Disorder (ASD)

The autism spectrum, as defined in the DSM-5 behavior diagnostic process, encompasses two primary domains:

1. Restricted and repetitive behavior, often characterized by a strong preference for consistency and sameness.
2. Difficulty with social and communicative behaviors, frequently accompanied by co-occurring issues like intellectual disability and language difficulties.

While technology and the Internet offer extensive opportunities for learning, communication, and recreation among children and young people, individuals with Autism Spectrum Disorder (ASD) may face increased vulnerability to certain risks. These risks include:

1. The Internet can provide children and young people with ASD the chance to engage in social interactions and explore special interests that might be less accessible in offline settings.
2. Challenges related to social interactions, such as difficulty in comprehending others' intentions, can render this group more susceptible to individuals with malicious intentions they may encounter online.
3. Online challenges often intersect with the core characteristics of autism. While clear and specific guidance can enhance the online experiences of individuals with ASD, the fundamental challenges associated with autism persist.

Children with disabilities

Children with disabilities encounter online risks similar to those faced by their non-disabled peers, but they may also confront specific risks related to their disabilities. These children often experience exclusion, stigma, and various barriers—physical, economic, societal, and attitudinal—that hinder their participation in their communities. Consequently, children with disabilities may seek social interactions and friendships in online spaces, which can have positive effects, such as building self-esteem and creating support networks. However, this online presence can also expose them to a higher risk of grooming, online solicitation, and sexual harassment. Research indicates that children encountering offline difficulties and those grappling with psychosocial challenges are more susceptible to such incidents[31].

In general, children who experience victimization offline are likely to face similar issues online. This heightened risk is especially pertinent for children with disabilities, who often have a greater need for online engagement. Studies demonstrate that children with disabilities are more prone to various forms of abuse, including sexual victimization. Such victimization may encompass bullying, harassment, exclusion, and discrimination based on their actual or perceived disabilities or related characteristics, such as their behavior, speech, or use of specialized equipment and services[32].

[31] Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content," Berkman Center for Internet & Society, Harvard University, December 2008, 87, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/%20files/ISTTF-LitReviewDraft_0.pdf.%E2%80%98
[32] UNICEF, "State of the World's Children Report: Children with Disabilities," 2013, https://doi.org/10.1177/0886260514534529.

Perpetrators of grooming, online solicitation, and sexual harassment targeting children with disabilities may consist of individuals who specifically target this group, including "devotees"—non-disabled individuals with a sexual attraction to people with disabilities, often those with amputations or mobility aids. Some of these individuals may even feign disabilities themselves[33]. Their actions can involve the downloading and sharing of seemingly innocuous photos and videos of children with disabilities through dedicated forums or social media accounts. The reporting tools on such platforms often lack appropriate mechanisms to address these actions.

Concerns also surround the practice of "sharenting," where parents share information and photos of their children online, potentially violating their privacy and exposing them to bullying or future negative consequences[34]. Parents of children with disabilities may engage in such sharing in search of support or advice, placing their children at a higher risk of adverse outcomes.

Certain children with disabilities may encounter challenges in using online environments or face exclusion due to inaccessible design, refusal of requested accommodations (e.g., screen reader software or adaptive computer controls), or the need for adequate support in navigating online interactions[35].

Regarding the acceptance of legal terms and conditions, children with disabilities are at an increased risk of agreeing to complex legal agreements that even some adults may struggle to comprehend.

Children's perceptions of online risks

Children worldwide express concerns about various online risks, including exposure to violence, access to inappropriate content and services, worries about excessive technology use, data protection, and privacy issues[36].

Adolescents, in particular, report a range of digital technology-related concerns. These encompass commonly discussed online safety issues like apprehensions about interacting with unfamiliar individuals on the internet, accessing unsuitable content, or encountering malware and viruses. Additionally, they express concerns about the reliability of their technology access, parental intrusion into their online privacy, and their level of digital literacy[37].

Research conducted by EU Kids Online indicates that in Europe, children's top online concerns revolve around pornography and violent content. Boys tend to be more perturbed by violent content, whereas girls are more focused on risks associated with online interactions. Concern levels appear to be higher among children from countries characterized as "high use, high risk."[38]

[33] Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder," Sexual and Disability 15, no. 4 (1997): 18, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.
[34] UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy," Innocenti Discussion Paper 2017-03 (UNICEF, Office of Research-Innocenti), accessed January 16, 2020, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.
[35] For guidelines on these rights, see the Convention on the Rights of Persons with Disabilities Article 9 on Accessibility and Article 21 on Freedom of expression and opinion, and access to information.
[36] Amanda Third et al., "Children's Rights in the Digital Age" (Melbourne: oung and Well Cooperative Research Centre, September 2014), http://www.uws.edu.au/%20data/assets/pdf_file/0003/753447/Childrens-rights-in%20-the-digital-age.pdf.
[37] Amanda Third et al., "Young and Online: Children's Perspectives on Life in the Digital Age," The State of the World's Children 2017 Companion Report (Sydney: Western Sydney University, 2017). The report summarized the views of 490 children aged 10–18, from 26 different countries speaking 24 official languages.
[38] Livingstone, S. (2014) EU Kids Online: Findings, methods, recommendations. LSE, London: EU Kids Online, https://lsedesignunit.com/EUKidsOnline/

In Latin America, consultations with children have revealed that privacy infringement, violence, and harassment are their primary concerns. Children report receiving unsolicited contact from unknown individuals, particularly when engaging in online gaming. To deal with such situations, their main strategy is to disengage and block the person. Girls, in particular, encounter harassment on social media platforms from an early age. They effectively navigate these forms of violence by blocking users and adjusting their privacy settings. Harassment sometimes originates from users who may not speak Spanish but can send them images, send friend requests, and comment on their posts. Some boys also report receiving such requests[39].

In many regions across the globe, children demonstrate a solid understanding of the online risks they face. Research has shown that the majority of children can differentiate cyberbullying from harmless joking or teasing online. They recognize that cyberbullying is characterized by a public dimension and an intent to cause harm[40].

PREPARING FOR A NATIONAL CHILD ONLINE PROTECTION STRATEGY

When formulating a national strategy for safeguarding children and adolescents on the internet to enhance their online security, the Royal Government of Bhutan (RGoB) and relevant policymaking bodies must recognize exemplary approaches and collaborate with essential participants. The subsequent sections delineate the standard participants and interested parties, along with a brief overview of their possible functions and duties concerning the protection of minors in the digital realm.

Actors and stakeholders

Policy-makers should identify appropriate individuals, associations, and entities representing these various actors and stakeholders within their jurisdiction. Understanding their existing, planned, and prospective initiatives is crucial for effective national coordination and implementation of strategies to safeguard children online.

Children and young people

Children and young people worldwide have demonstrated their adeptness at adapting to and utilizing new technologies effortlessly. The Internet is progressively gaining importance in educational settings, serving as a space where children can engage in learning, leisure, and communication.

In accordance with the recent report from ChildFund Alliance, merely 18.1 percent of interviewed children believe that governing authorities take actions to safeguard them. Policy-makers should actively involve children in these matters, acknowledging their right to express their views as articulated in Article 12 of the UN Convention on the Rights of the Child (UNCRC).

For effective child protection, policy-makers should establish a standardized definition of a child in all legal documents, defining a child as an individual below the age of 18. This definition aligns with Article 1 of the UNCRC, which defines a child as "every human being below the age of 18 years." It is imperative that companies are not permitted to treat individuals under 18, who are legally old enough

[39] Contectados al Sur network, "Hablatam."
[40] UNICEF, "Global Kids Online Comparative Report (2019)."

to consent to data processing, as adults. This narrow definition lacks substantiation based on evidence of childhood developmental milestones and jeopardizes the rights and safety of children.

Despite many children demonstrating confidence in using technology, a significant number feel unsafe online and harbor numerous concerns about the Internet[41]. Children's limited experience of the broader world makes them susceptible to various risks, and they have a legitimate expectation of assistance and protection. Additionally, it's crucial to recognize that not all children and young people will encounter the Internet or new technologies in the same manner. Some children with specific needs stemming from physical or other disabilities may be especially vulnerable in the online environment and require additional support.

Repetitive surveys have indicated disparities between what adults believe children and young people do online and the actual occurrences. Half of all surveyed children expressed that adults in their countries do not listen to their opinions on relevant matters. Therefore, it is imperative that any national-level arrangements devised for policy development in this domain incorporate suitable mechanisms to facilitate the expression of all children's and young people's perspectives and account for their real experiences in using technology[42].

Parents, guardians, and educators

Parents, guardians, and educators assume the primary responsibility for children's well-being and should receive digital literacy education to comprehend the online landscape. This knowledge will enable them to safeguard children and impart essential online safety skills.

Educational institutions bear a distinct obligation to educate children on online safety, regardless of whether they are using the Internet in school, at home, or elsewhere. National curricula should incorporate digital literacy from an early age, spanning from 3 to 18 years old. This approach equips children with the capacity to protect themselves, be aware of their rights, and harness the Internet for educational purposes[43].

Policy-makers must recognize that parents and guardians serve as the initial, ultimate, and most effective line of defense and support for their children. However, many of them may feel uncertain when it comes to the Internet. Schools can serve as a vital avenue for reaching out to parents and guardians, informing them about both the risks and the myriad positive opportunities offered by new technologies. Nevertheless, diversifying communication channels is essential to maximize outreach to a broader audience. Industry players also have a significant role in assisting their users or customers. Parents and guardians may opt to oversee their child's online activities, engage in conversations about proper behavior and technology usage, and gain insights into their child's online actions to merge the online and offline experiences seamlessly within family discussions.

Furthermore, parents and guardians must exemplify good practices for their children in terms of device usage and appropriate online behavior.

[41] Council of Europe, "It's Our World: Children's Views on How to Protect Their Rights in the Digital World," Report on child consultations (Council of Europe, Children's Right Division, October 2017.
[42] Child Fund Alliance, "VIOLENCE AGAINST CHILDREN AS EXPLAINED BY CHILDREN," Save Voices Big Dreams, 2019, https://child-fundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee81cb216/SVBD-THE_REPORT-digital.pdf
[43] UNICEF, "Policy Guide on Children and Digital Connectivity" (Policy Lab, Data, Research and Policy, United Nations Children's Fund, June 2018), https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf.

Policy-makers should remember the importance of consulting parents and caregivers to gather their perspectives, experiences, and comprehension of online child protection.

Lastly, policy-makers, in conjunction with other public institutions, can devise public awareness campaigns aimed at parents, caregivers, and educators. Public libraries, healthcare centers, shopping malls, and major retail venues can all serve as accessible platforms for disseminating e-safety and digital skills information. Governments must ensure that this endeavor provides impartial advice devoid of private interests and encompasses a wide array of digital space-related topics.

Industry

The industry constitutes a crucial stakeholder within the ecosystem due to its possession of technological expertise that policy-makers require to comprehend and address in the formulation of legal frameworks for child online protection. Therefore, it is imperative that policy-makers engage the industry during the development of laws pertaining to child online protection.

Furthermore, it is essential to encourage the industry to adopt a safety by design approach in their business operations when creating new technology. It is evident that companies involved in the development or provision of new technology products and services should assist their users in comprehending the functioning and safe and appropriate usage of these technologies.

The industry also bears significant responsibility in advancing awareness of online safety, particularly among children, their parents or guardians, and the broader community. By engaging in such efforts, industry stakeholders can gain a deeper understanding of concerns from other stakeholders and the potential risks and harms faced by end users. Armed with this knowledge, the industry can rectify existing products and services and identify hazards during the development phase.

Recent advancements in artificial intelligence are opening up opportunities for the industry to incorporate more robust checks and balances to verify users' identities and create a conducive online environment for positive behavior among children. However, these advancements may also introduce new risks to children.

In certain nations, the Internet operates within a framework of self-regulation or co-regulation. Nevertheless, some countries are contemplating or have implemented legal and regulatory frameworks that impose obligations on companies to detect, block, and/or remove harmful content targeting children from their platforms or services. Additionally, these frameworks may mandate the provision of clear reporting channels and access to support.

The research community and non-governmental organizations

Within the academic and research communities, it is highly probable that there exist numerous scholars and experts who possess professional interests and extensive knowledge concerning the social and technical impacts of the Internet. These individuals represent a highly valuable asset for RGoB and policy-makers in the development of evidence-based strategies. They can contribute by providing substantiated facts and robust evidence, serving as a counterbalance to business interests that may sometimes prioritize short-term commercial gains.

Likewise, within the non-governmental organization (NGO) sector, a diverse range of expertise and information is available. This expertise serves as an invaluable resource for outreach efforts and the provision of services to children, parents, caregivers, and educators, promoting the online safety agenda and safeguarding the broader public interest.

Law enforcement

Regrettably, technology, while offering numerous benefits, has also drawn the attention of criminal and antisocial elements. The Internet has significantly amplified the dissemination of Child Sexual Abuse Material (CSAM) and various other online harms. Predators have exploited the Internet to initiate contact with children, enticing them into harmful forms of interaction, both online and offline. Cyberbullying and other forms of harassment can inflict substantial harm on the lives of children, and the Internet has provided new avenues for such harm to occur.

Therefore, it is imperative that the law enforcement community fully engages with any comprehensive strategy aimed at enhancing online safety for children and young people. Law enforcement officers should receive appropriate training to conduct investigations into Internet-related crimes involving children and young people. They require a requisite level of technical expertise and access to forensic resources, enabling them to efficiently extract and interpret data acquired from computers or the Internet.

Furthermore, it is crucial for law enforcement to establish clear mechanisms allowing children, young people, and the general public to report incidents or concerns related to online safety for children and young people. Many countries have implemented hotlines to facilitate reporting of CSAM, and similar dedicated mechanisms exist for reporting other issues, such as bullying. Policy-makers should collaborate with the International Association of Internet Hotlines (INHOPE), supporting their efforts in assessing and processing CSAM reports and benefiting from INHOPE's assistance in helping organizations worldwide establish hotlines where none exist. Policy-makers should ensure open lines of communication between law enforcement and other stakeholders.

Law enforcement plays a central role in addressing CSAM seized within national borders, necessitating the establishment of processes to examine this material to identify potential local victims. In cases where identification is not possible, the material should be forwarded to INTERPOL for inclusion in the ICSE Database. Given the global nature of this threat, policy-makers should promote international cooperation among law enforcement agencies worldwide, streamlining formal processes and enabling quicker responses.

Social services

In cases where children or young people have experienced harm or abuse online, such as the posting of inappropriate or illegal images of them, it is highly probable that they will require specialized and long-term support or counseling. Additionally, there may be a necessity for comprehensive services and restorative practices for offenders, particularly in cases involving young offenders who may have also been victims of online or offline abuse. Professionals within the social services sector must undergo suitable training to be equipped to offer this type of assistance. This support should be delivered through both online and offline channels, catering to the specific needs and circumstances of the individuals involved.

Health care services

Healthcare services required following any incident of violence against a child should be included within the national-level basic healthcare plan. Healthcare institutions must have mechanisms for mandatory reporting of abuse in place. Furthermore, healthcare professionals should receive appropriate training and possess the necessary knowledge to offer support to children in such situations. Healthcare services should encompass assistance for children's mental health and overall well-being, ensuring comprehensive care for those affected by violence.

Government Ministries

The Child Online Protection policy spans various Government Ministries/Agencies, and it is crucial to involve all of them in the development of a successful national strategy and action plan. These entities may encompass:

- Ministry of Home Affairs
- Ministry of Health
- Ministry of Education and Skills Development
- Office of the Attorney General
- Government Technology Agency (GovTech Agency)

Regulatory bodies

Regulatory authorities, including those responsible for media and data protection, are well-suited to fulfill the roles of overseers and coordinators in collaboration with government institutions.

Broadband, mobile, and Wifi network operators

Service providers have the responsibility to identify, restrict, and report unlawful content within their network while offering user-friendly tools, services, and settings that assist parents in controlling their children's access. It is vital for providers to maintain a balance, ensuring that both individual freedoms and privacy are upheld.

Children's Rights

Independent human rights organizations dedicated to children can play a vital role in ensuring the online safety of children. Although the specific tasks of these institutions may vary, they often include functions such as:

- Monitoring how laws, policies, and practices impact children's rights protection.
- Promoting the implementation of global human rights standards at the national level.
- Investigating violations of children's rights.
- Offering expertise on children's rights to the legal system.

- Ensuring that children's perspectives are considered in matters concerning their human rights, including the development of relevant laws and policies.
- Raising public awareness about children's rights.
- Conducting human rights education and training programs.

It is crucial to involve children directly, as their right under Article 12 of the UNCRC dictates. Independent human rights institutions for children can perform advisory, investigative, awareness-raising, and educational roles, all of which are relevant for preventing and addressing the harm children may encounter online. Therefore, these institutions should be central to the development of a comprehensive, rights-based approach to enhancing the legal, regulatory, and policy frameworks related to child online protection. This approach should also include direct consultations with children, as mandated by Article 12 of the UNCRC.

In recent times, some jurisdictions have established or considered the creation of state agencies with a specific mission to support children's rights online, particularly in protecting them from violence or harm. If such agencies exist, they should also be closely involved in efforts to strengthen child online protection at the national level.

Existing responses for child online protection

Numerous initiatives have been established to address the growing significance of ICTs in the lives of children globally, as well as the associated risks faced by the youngest members of our societies, both at the national and international levels.

National models

Nationally, there are several legislations that deserve attention for their role in addressing critical aspects of a comprehensive framework for Child Online Protection. These legislations include, but are not limited to:

- Audiovisual Media Services Directive (AVMSD) (subject to review in 2018, EU).
- General Data Protection Regulation (GDPR) (implemented in 2018, EU).

In recent years, member states have demonstrated innovative approaches in their regulatory and institutional responses to threats affecting the safety and well-being of children online. It's important to note that there is no one-size-fits-all solution to challenges such as child sexual abuse material (CSAM), cyberbullying, and other online harms faced by children. However, noteworthy new approaches have been tested in the past few years, including:

1. **The Age-Appropriate Design Code (2019, UK):** In early 2019, the Information Commissioners Office introduced proposals for the 'age-appropriate design code' to enhance child protection online. This code prioritizes the best interests of the child, aligning with the UNCRC principles. It outlines several expectations for the industry, such as robust age-verification measures, default settings that turn off location services for children, minimal collection and retention of children's personal data, safety considerations in product design, and age-appropriate and accessible explanations.

2. **The Harmful Digital Communications Act (reviewed in 2017, New Zealand):** This 2015 legislation addresses a wide range of digital harms, including cyberbullying and revenge porn. Its aim is to discourage, prevent, and mitigate harmful digital communications. The act makes it illegal to post digital communications with the intent of causing severe emotional distress to others and establishes ten communication principles. It empowers users to report violations to an independent organization and seek court orders against communication authors or hosts if issues are not resolved.

The eSafety Commissioner (established in 2015, Australia): The eSafety Commissioner is the world's first government agency dedicated exclusively to online safety. Established in 2015, it has a legislative mandate to lead, coordinate, educate, and provide advice on online safety to ensure safe and positive online experiences for all Australians. The eSafety Commissioner oversees investigative schemes that target various harms, including serious cyberbullying of children, image-based abuse, and prohibited content. It has the authority to investigate and take action on complaints or reports related to these harms, including issuing removal notices to individuals and online services. In addition to its investigative powers, eSafety employs a holistic community approach that encompasses social, cultural, and technological initiatives to promote online safety comprehensively. Its efforts encompass prevention, protection, and proactive measures to ensure online safety.

International models

Internationally and across borders, various recommendations and standards have been established by different stakeholders, building upon the efforts of the following initiatives:

1. Guidelines related to the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography.
2. Council of Europe Guidelines designed to respect, protect, and fulfill children's rights in the digital environment. These guidelines are directed towards all member states of the Council of Europe, aiming to assist them and other relevant stakeholders in adopting a comprehensive, strategic approach to maximize children's rights in the digital realm. These guidelines cover a wide range of topics, including personal data protection, child-friendly content tailored to their evolving capacities, helplines and hotlines, vulnerability and resilience, and the roles and responsibilities of business enterprises. Moreover, they emphasize the importance of engaging with children in decision-making processes to ensure that national policies effectively address digital environment developments. These guidelines are available in 19 languages and are expected to be complemented by a child-friendly version of the document and a Handbook for policy-makers, offering practical measures for guideline implementation[44].
3. Council of Europe's Lanzarote Convention, the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, which mandates States to provide a comprehensive response to sexual violence against children through the "4ps approach" encompassing Prevention, Protection, Prosecution, and Promotion of national and international cooperation. The Lanzarote Committee, responsible for overseeing the Convention's operation in the digital environment, has issued various documents to clarify its application. These documents include an Opinion on child sexually suggestive or explicit images and videos generated, shared, and

[44] Council of Europe (2020), The Digital Environment, https://www.coe.int/en/web/children/the-digital-environment.

received by children, an Interpretative Opinion on the Convention's applicability to sexual offenses against children facilitated through the use of ICTs, a Declaration on web addresses advertising child sexual abuse material or related offenses under the Lanzarote Convention, and an Opinion on Article 23 of the Lanzarote Convention addressing solicitation of children for sexual purposes through information and communication technologies (Grooming). The Lanzarote Committee conducts monitoring of the Convention's implementation, with the second thematic monitoring round focusing on the protection of children against sexual exploitation and sexual abuse facilitated by ICTs.

4. Additional Council of Europe guidelines, standards, and tools contribute to a collective framework designed to address various aspects. The Council of Europe's Convention on Cybercrime obligates Parties to criminalize offenses related to child sexual abuse material and is ratified by 64 States Parties. The Council of Europe also places emphasis on empowering children and their surroundings to safely navigate the digital sphere through educational tools, including the Internet Literacy Handbook (2017), Digital Citizenship Education Handbook (2019), and manuals for parents. Additionally, the Council of Europe conducts research involving children to understand their views on protecting their rights in the digital environment and has undertaken consultative research focused on children with disabilities' experiences in the digital realm[45].

Child Online Safety Report

The Child Online Safety Report, titled "Child Online Safety: Minimizing the Risk of Violence, Abuse, and Exploitation Online," along with the Child Online Safety Universal Declaration, represent significant international efforts aimed at reducing the dangers associated with violence, abuse, and exploitation of children on the internet.

Additionally, the OECD (Organization for Economic Co-operation and Development) Recommendations on the Protection of Children Online, initially established in 2012 and subject to review in 2019-2020, play a crucial role in setting guidelines for safeguarding children online. These recommendations are valuable not only at the national level but also support international cooperation efforts in establishing child online protection strategies.

Furthermore, several other national and transnational initiatives contribute to international collaboration and assist individual countries in their endeavors to create effective child online protection strategies:

1. The International Child Sexual Exploitation Image Database (ICSE DB), overseen by INTERPOL, serves as a robust intelligence and investigative tool, facilitating data sharing among specialized investigators globally. Accessible through the secure INTERPOL police communications system (I-247), this database employs advanced image comparison software to establish connections among victims, perpetrators, and locations. Certified users from member countries can utilize the ICSE DB in real-time for various investigative tasks related to child sexual exploitation cases.
2. The WePROTECT Global Alliance (WPGA) represents a global movement that unites governments, major technology companies, and civil society organizations to address online child sexual exploitation (OSCE) worldwide. Distinguished by its multi-stakeholder approach,

[45] ITU, 2020, Guidelines for Policy-makers on Child Online Protection, https://www.itu-cop-guidelines.com/

the WPGA aims to enhance victim identification and protection, apprehend offenders, and ultimately eradicate online child sexual exploitation. It encompasses key components, including a Model National Response and a Global Strategic Response.

3. The DQ Institute's 2020 Child Online Safety Index (COSI) is a groundbreaking real-time analytical platform designed to assist nations in monitoring the state of online safety for their children. The COSI framework is based on six pillars: Cyber Risks, Disciplined Digital Use, Digital Competency, Guidance and Education, Social Infrastructure, and Connectivity. These pillars cover a broad spectrum of aspects related to children's online safety, encompassing responsible technology use, empowerment, and necessary infrastructure[46].

These initiatives collectively contribute to international and national efforts to ensure the safety and well-being of children in the digital age.

Benefits of a national child protection strategy

Harmonisation of laws

The adoption of appropriate legislation by all countries to combat the misuse of ICTs for criminal or illicit purposes is a fundamental aspect of achieving global cybersecurity. Cyber threats can originate from anywhere worldwide, making these challenges inherently international in nature. Addressing them necessitates international collaboration, mutual assistance in investigations, and the establishment of shared legal provisions and procedures. Therefore, it is essential for countries to align their legal frameworks to combat cybercrime, protect children online, and facilitate international cooperation.

Developing comprehensive national legislation, including a framework to combat cybercrime, is a crucial step in the success of any national strategy for child online protection. This involves creating substantive criminal laws that criminalize activities such as computer fraud, illegal access, data interference, copyright infringements, and the distribution of CSAM. It is equally important to ensure that these legal provisions do not unfairly criminalize children. While some existing criminal code provisions may apply to similar real-world offenses, they may not be directly applicable to cybercrimes. Therefore, it is imperative to conduct a thorough assessment of current national laws to identify any gaps in addressing cybercrimes effectively.

The subsequent phase involves defining legislative language and reference materials to guide countries in formulating harmonized cybercrime laws and procedural rules. These practical tools can assist nations in developing a legal framework for cybersecurity and related legislation. The ITU has actively collaborated with its Member States and relevant stakeholders in advancing the global harmonization of cybercrime laws.

Given the rapid pace of technological advancement, self-regulation and co-regulation have been proposed as potential solutions to adapt to evolving challenges in online child protection, as traditional legislative processes can be time-consuming and risk becoming obsolete. However, for these measures to be effective, regulators and policy-makers should clearly define child online protection objectives and challenges. They should also establish a transparent review process and assessment

[46] Broadband Commission for Sustainable Development (2019), The State of Broadband 2019: Broadband as a Foundation for Sustainable Development, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

methodology to evaluate the effectiveness of self-regulation and co-regulation. In cases where these mechanisms prove insufficient in addressing identified challenges, policy-makers should initiate a formal legislative process to rectify the situation. Furthermore, successful self-regulatory measures can gradually be incorporated into formal laws through the legislative process to serve as a legal framework and ensure the sustainability of these initiatives[47].

Coordination

It is probable that among the various actors and stakeholders, there are already numerous ongoing initiatives and actions aimed at safeguarding children online. However, these efforts have often operated independently. Recognizing and comprehending these existing activities is crucial in assessing the current landscape of child online protection.

The national child online protection strategy aims to serve as a unifying framework that will harmonize and guide these disparate efforts. It will coordinate and channel the collective energy of both existing and novel activities toward a common goal, ensuring a more cohesive and effective approach to protecting children in the online environment.

RECOMMENDATIONS FOR FRAMEWORKS AND IMPLEMENTATION

Governments must address all forms of violence against children occurring in the digital realm. However, while implementing measures to safeguard children online, it is essential to ensure that these actions do not unreasonably limit the exercise of other fundamental rights, such as the right to freedom of expression, the right to access information, or the right to freedom of association. Instead of stifling children's inherent curiosity and innovative spirit out of concern for online risks, it is imperative to harness their ingenuity and bolster their resilience as they explore the potential of the digital environment.

In many instances, acts of violence against children are perpetrated by their peers. In such cases, governments should prioritize restorative approaches that aim to mend the harm caused, all while avoiding the unnecessary criminalization of children. Governments should actively promote the utilization of ICTs in both preventing and addressing instances of violence. This includes the development of technologies and resources that empower children to access information, block harmful content, and report incidents of violence when encountered[48].

To effectively address the global issue of child online safety, governments must facilitate communication and cooperation among relevant entities within their jurisdictions. Open and collaborative efforts are necessary to eradicate harm to children in the online sphere.

Framework recommendations

Legal Framework

Governments should conduct a thorough review of their legal framework and make necessary updates to ensure the full protection of children's rights in the digital environment. A comprehensive

[47] Broadband Commission for Sustainable Development (2019)
[48] Special Representative of the Secretary-General on Violence against Children, Annual Report of the Special Representative of the Secretary-General on Violence against Children to the Human Rights Council, A/ HRC/31/20 (January 2016), para. 103 and 104.

legal framework should encompass various elements, including preventive measures, the prohibition of all forms of violence against children online, the provision of effective remedies, recovery, and reintegration mechanisms for addressing violations of children's rights. Additionally, it should establish child-friendly counseling services, reporting and complaint mechanisms, as well as accountability measures to combat impunity[49].

Whenever possible, legislation should be crafted to be technology-neutral, ensuring its relevance and applicability in the face of future technological advancements[50].

Effective implementation of these legal provisions necessitates the implementation of complementary measures, such as awareness-raising initiatives, social mobilization campaigns, educational efforts, and capacity-building programs for professionals working with and for children.

While developing appropriate laws, policy-makers should consider that children are not a homogenous group, and different responses may be required based on factors like age, specific needs, or heightened risks in the digital environment.

Governments should establish a clear and predictable legal and regulatory framework that supports businesses and other third parties in fulfilling their responsibilities to protect children's rights in all aspects of their operations, both domestically and internationally[51].

In reviewing the scope of legal frameworks, policy-makers should consider provisions related to:

- Grooming or other forms of remote enticement, extortion, or coercion of children into inappropriate sexual contact or activity.
- Ensuring the possession, production, and distribution of child sexual abuse material (CSAM), regardless of the intent to distribute.
- Addressing online harassment, bullying, abuse, or hate speech.
- Combating online terrorist material.
- Enhancing cybersecurity measures.
- Reflecting that actions deemed illegal offline are equally unlawful online.

Policy and institutional frameworks

Ensuring that children's rights in the digital realm are safeguarded requires governments to strike a delicate balance between maximizing the advantages of children's ICT usage and minimizing associated risks. Achieving this balance entails incorporating measures for online child protection into national broadband plans and formulating a comprehensive child online protection strategy[52]. This strategy should be seamlessly integrated into existing policy frameworks pertaining to children's rights and child protection, complementing national child protection policies by offering a dedicated framework

[49] Special Representative of the Secretary-General on Violence against Children, Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children, 2014 (New York: United Nations), p. 55.
[50] Special Representative of the Secretary-General on Violence against Children, Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children, 2014 (New York: United Nations),p.64
[51] UN Committee on the Rights of the Child, General Comment No. 16, para. 53.
[52] The State of the Broadband 2019, Recommendation 5.6, page 78. https://www.itu.int/dms_pub/itu-s/opb/%20pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

that addresses all potential risks and harms faced by children, with the ultimate goal of creating a secure, inclusive, and empowering digital environment[53].

Governments should establish a national coordinating framework endowed with a clear mandate and sufficient authority to oversee all activities concerning children's rights and digital media and ICTs. This coordinating body should operate across various sectors, encompassing national, regional, and local levels. It should also include specific time-bound objectives and a transparent mechanism for evaluating and monitoring progress. Adequate human, technical, and financial resources must be allocated to ensure the effective functioning of this framework[54].

Furthermore, governments should create a multi-stakeholder platform tasked with guiding the development, implementation, and monitoring of the national digital agenda for children. This platform should bring together representatives from various key constituencies, including children and youth, parent and caregiver associations, relevant government departments, education, justice, health, and social care sectors, national human rights institutions, regulatory bodies, civil society, industry, academia, and relevant professional associations.

Regulatory framework

Governments bear responsibility for instances where business enterprises have infringed upon children's rights, especially when they have not taken the necessary, appropriate, and reasonable measures to prevent or address such violations, or when they have collaborated with or tolerated such infringements[55].

The Guiding Principles on Business and Human Rights stipulate that corporations should establish redress and grievance mechanisms that adhere to several principles, including legitimacy, accessibility, predictability, fairness, compatibility with human rights, transparency, dialogue-based, and conducive to learning. These mechanisms established by businesses can offer flexible and timely resolutions, and in some cases, it may be in the best interest of a child for concerns about a company's conduct to be addressed through these mechanisms. However, access to courts or judicial review of administrative remedies and other procedures should always remain available. Consideration should also be given to creating mechanisms that provide safe and age-appropriate channels for children to report their concerns[56].

Apart from internal grievance mechanisms, governments should establish monitoring mechanisms to investigate and remedy violations of children's rights. This will enhance accountability among ICT and relevant companies and strengthen the regulatory agencies' role in setting standards related to children's rights and ICTs[57]. This is particularly important because other remedies, such as civil proceedings and judicial redress, can often be cumbersome and costly[58].

[53] For model provisions on child protection for national broadband plans see chapter 10 of the Child Online Safety Report.
[54] Special Representative of the Secretary-General on Violence against Children, Annual Report of the Special Representative of the Secretary-General on Violence against Children (December 2014) A/HRC/28/55 and Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children, 2014 (New York: United Nations), para. 88.
[55] UN Committee on the Rights of the Child, General Comment No. 16, para. 28.
[56] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, A/HRC/17/31 (2011), para. 71.
[57] UN Committee on the Rights of the Child, Report of the 2014 Day of General Discussion, para. 96.
[58] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016), para. 71.

The UN Committee on the Rights of the Child has highlighted the potential role of national human rights institutions in this regard, suggesting that they can receive, investigate, and mediate complaints against industry entities, conduct public inquiries into large-scale abuses, and review legislation to ensure compliance with children's rights. These institutions should ensure child sensitivity, protect victims' privacy, and engage in monitoring, follow-up, and verification for child victims.

For instance, in cases of cyberbullying where internal remedial mechanisms may prove ineffective, empowering a public authority to receive complaints and intervene with content hosts to remove harmful material would be a crucial safeguard for children. This approach offers the advantage of a swift response, which is essential in addressing cyberbullying, and provides a clear legal basis for removing such content[59].

While framing regulatory approaches for the digital environment, governments must also consider the impact of such regulation on the enjoyment of all human rights, including freedom of expression[60].

Governments should place an obligation on businesses to conduct due diligence related to children's rights, ensuring that enterprises identify, prevent, and mitigate any adverse impact on children's rights across their business relationships and global operations[61]. Additionally, governments should contemplate additional measures, such as requiring industry entities that may impact children's rights in the digital realm to adhere to the highest standards for preventing and addressing potential rights violations in order to qualify for funding or contracts.

Recommendations for implementation

Governments must offer assistance to help child victims seek prompt and appropriate reparation for the harm they have suffered, including the possibility of compensation when deemed suitable. Moreover, governments should provide comprehensive support and aid for child victims of violations related to digital media and ICTs, ensuring their complete recovery and reintegration while preventing their re-victimization.[62]

To facilitate this, governments should establish child-sensitive counselling, reporting, and complaint mechanisms, such as helplines, through legal frameworks. These mechanisms should be integrated into the national child protection system, ensuring a streamlined process for children seeking assistance during distressing times. Helplines, in particular, are invaluable for addressing highly sensitive issues like sexual abuse, which children may find challenging to discuss with peers, parents, caregivers, or teachers. Helplines also play a vital role in guiding children to essential services like legal support, safe housing, law enforcement, or rehabilitation[63].

Additionally, governments should focus on understanding and monitoring the behavior of offenders to improve detection rates of abusers and reduce the risk of convicted offenders re-offending. Establishing helplines that offer free and anonymous phone or chat-based counseling and support for individuals

[59] Bertrand de Crombrugghe, "Report of the Human Rights Council on Its Thirty-First Session" (UN Human Rights Council, 2016).
[60] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016), para. 45.
[61] UN Committee on the Rights of the Child, General Comment No. 16, para. 62.
[62] UN Committee on the Rights of the Child, Report of the 2014 Day of General Discussion, para. 106.
[63] Special Representative of the Secretary-General on Violence against Children, Releasing children's potential and minimizing risks, p. 51 and p. 65.

experiencing inappropriate feelings or thoughts toward children, potentially preventing offending behavior, is essential. Assisting offenders in changing their behavior can significantly minimize the risk of reoffending.

Statutory complaint-handling mechanisms are another essential component of an effective remedial framework. Regulators should conduct independent assessments and studies to evaluate how platforms address child protection issues. There are technological solutions available for regulators to independently monitor platforms, and the industry should be encouraged to publish transparency reports. Collaboratively with the international community and the industry, governments should develop a universal set of metrics that stakeholders can use to evaluate various aspects of child online safety comprehensively.

Sexual exploitation

Concrete considerations for policy-makers when addressing threats and harms to children, including child sexual abuse material (CSAM), self-generated content, grooming, sextortion, and other online risks, may include:

1. Implementing measures to disrupt or decrease the circulation of CSAM, such as establishing a national hotline or utilizing an IWF Reporting Portal, along with deploying methods to block access to online content known to contain or promote CSAM.
2. Establishing national processes to channel all CSAM discovered within a country to a centralized national resource with legislative authority to instruct companies to remove the content.
3. Developing strategies to tackle the demand for CSAM, especially among individuals with prior convictions for such offenses. Raising awareness about the non-victimless nature of this crime, emphasizing that children are abused to create the material, and holding individuals criminally accountable for viewing or downloading CSAM.
4. Promoting the understanding that children can never consent to sexual abuse, whether for CSAM production or any other purpose. Encouraging individuals who use CSAM to seek help while making them aware of their criminal liability for engaging in illegal activities.
5. Exploring other strategies to address the demand for CSAM, such as maintaining registers of convicted sex offenders and potentially integrating these lists into block lists to restrict their access to specific websites frequented by children and young people.
6. Ensuring appropriate long-term support for victims who have been victimized online, including those whose illegal images have surfaced on the Internet. Such support should be available on an extended basis to address their vulnerability to bullying and further exploitation.
7. Establishing and promoting a mechanism for reporting illegal content or concerning online behavior, similar to systems implemented by organizations like the Virtual Global Taskforce and INHOPE. Encouraging the use of the INTERPOL i24/7 system for reporting.
8. Providing sufficient training for law enforcement officials to investigate internet and computer-based crimes effectively, along with access to appropriate forensic facilities for extracting and interpreting digital data.

9. Investing in training for law enforcement, prosecutorial, and judicial authorities to understand the methods employed by online criminals. Additionally, acquiring and maintaining the necessary facilities for digital forensics evidence retrieval and interpretation is crucial. Establishing collaborative information exchanges with relevant law enforcement agencies in other countries is also essential for addressing these crimes effectively.

Education

Educating children on digital literacy should be an integral part of a comprehensive strategy aimed at ensuring their safe and beneficial use of technology. This education equips children with critical thinking skills necessary to discern both positive and negative aspects of their online behavior. While it's essential to convey the potential harms of online activities to children, this should be just one component of a broader digital literacy program, tailored to their age and focused on developing practical skills and competencies.

Incorporating social and emotional learning concepts into online safety education is crucial, as it helps students understand and manage their emotions, fostering healthy and respectful relationships in both the online and offline realms.

Empowering children with appropriate tools and knowledge to navigate the Internet is paramount for their safety. One effective approach is integrating digital literacy into school curricula. Alternatively, educational resources can be developed outside the school curriculum to ensure comprehensive coverage.

Professionals working with children should possess the requisite knowledge and skills to effectively assist children in responding to and resolving issues related to child online protection. Additionally, they should impart the digital skills necessary for children to harness the benefits of technology successfully.

Industry

National and international industry stakeholders have a crucial role to play in raising awareness about child online safety issues. Their efforts should extend to educating all adults responsible for a child's well-being, including parents, caregivers, schools, youth-serving organizations, and communities, by providing them with the necessary knowledge and skills to ensure children's safety. Industry players should adopt a "safer by design" approach, prioritizing safety as a fundamental objective in their products, services, and platforms.

To contribute to child online safety, industry should take the following actions:

1. Develop age-appropriate and family-friendly tools to assist users in effectively managing online safety for their families.
2. Establish suitable reporting mechanisms for users to report issues and concerns, with an expectation of timely responses that include information about actions taken. Additionally, proactive reporting of child abuse incidents should be implemented to detect and address criminal activities against children.

3. Implement measures to prevent platform exploitation, such as utilizing services like the Internet Watch Foundation (IWF Services), to ensure a cleaner and safer online environment.

It is essential to ensure that all relevant stakeholders within the ecosystem are aware of online risks and potential harms to prevent unnecessary risks to children.

Moreover, there is a need to develop common metrics for child online safety to comprehensively measure various aspects of the issue. These common standards and metrics are essential for tracking progress at the national and international levels, evaluating the success of projects and activities aimed at eliminating violence against children online, and recognizing the effectiveness of the child online safety ecosystem.

DEVELOPING A NATIONAL CHILD ONLINE PROTECTION STRATEGY

A national checklist

In order to formulate a national strategy focusing on online child safety, policy-makers need to consider a range of strategies. Table 1 sets out key areas for consideration.

	Sl. No.	Key areas for consideration	Description
Legal framework	1.	Examine the current legal framework to ensure that it possesses all the essential legal authorities required to empower law enforcement and other pertinent agencies to safeguard individuals below the age of 18 across all Internet-enabled platforms.	In most cases, it's essential to establish a comprehensive set of laws that explicitly state that any crime against a child that exists in the physical world can also occur on the Internet or any electronic network, with necessary adaptations. Furthermore, there may be a need to create new laws or modify existing ones to prohibit specific online behaviors that are unique to the Internet, such as enticing children remotely to engage in or watch sexual activities or grooming children for in-person sexual purposes. In addition to these objectives, it's generally important to have a legal framework that condemns the misuse of computers for criminal purposes, including hacking or other unauthorized use of computer code, while recognizing that the Internet can be a platform for criminal activities.
	2.	Ensure that, with necessary adjustments, any action targeting a child, which is considered unlawful in the physical world, is equally illegal in the online realm, and that the regulations concerning online data protection and privacy for children are sufficient.	

Regulatory framework	3.	Consider the development of regulatory policies, which can encompass either a self-regulation or co-regulation approach, as well as a comprehensive regulatory framework. The self-regulation or co-regulation model may involve the creation and publication of guidelines for best practices or fundamental online safety standards. This approach serves to facilitate and maintain the participation of all relevant stakeholders and enables faster responses to technological advancements. On the other hand, a regulatory model would establish clear expectations and responsibilities for all stakeholders within a legal framework. Potential penalties for violations of these policies could also be contemplated.	Certain nations have adopted a self-regulatory or co-regulatory approach to policy development in this domain. Through such approaches, they have issued guidelines of best practices to offer guidance to the internet industry regarding effective measures for enhancing online safety for children and young individuals. For instance, in the European Union, EU-wide codes have been released for both social networking platforms and mobile phone networks, outlining guidelines for providing content and services to children and young people over their networks. The advantage of self and co-regulation lies in their agility, allowing for a quicker response to technological advancements. More recently, several countries have moved towards the establishment and implementation of a regulatory framework. In these instances, the regulatory framework has evolved from self or co-regulatory models and outlines the obligations and anticipations for stakeholders, particularly industry providers, to enhance the protection of their users.
Reporting - illegal content	4.	Establish and widely publicize a user-friendly mechanism for reporting diverse forms of illegal content discovered on the Internet. This could involve the creation of a national hotline with the capability to swiftly respond and take action to remove or restrict access to illicit materials. Industry entities should implement mechanisms to detect, prevent, and eliminate instances of child exploitation online, covering all services relevant to their organizations.	Promote and publicize mechanisms designed for reporting instances of online abuse or objectionable/ illegal behavior. These reporting avenues should be widely advertised across the Internet and through various media channels. In cases where a national hotline is unavailable, an alternative like the IWF Reporting Portals can serve as a solution. Ensure that links to report abuse mechanisms are conspicuously displayed on relevant sections of websites that allow user-generated content. Additionally, individuals who feel threatened or witness concerning online activities should have the means to quickly report them to law enforcement agencies that should be adequately trained and prepared to respond. The Virtual Global Taskforce is a law enforcement entity offering a 24/7 reporting mechanism for illegal content or behavior. It is accessible to individuals in the USA, Canada, Australia, and Italy, with other countries expected to join soon. More information can be found at www.virtualglobaltaskforce.com. Also, reference INHOPE.
Reporting - user concerns	5.	Industry should offer users the ability to report any concerns or issues they encounter and take appropriate actions in response to these reports.	Service providers must be required to offer their users clear and easily accessible mechanisms to report problems and concerns within their services, and these mechanisms should be designed to be child-friendly.

Actors and stakeholders	6.	Engage all relevant stakeholders interested in online child protection, including: • Government agencies • Law enforcement • Social services organizations • Internet Service Providers (ISPs) and other Electronic Service Providers (ESPs) • Mobile phone network providers • Public Wi-Fi providers • Other pertinent technology companies • Teacher associations • Parent associations • Children and young people • Child protection and related NGOs • Academic and research communities • Owners of public access providers, such as Internet cafes, libraries, telecentres, PC Bangs, and online gaming centers, among others.	Several national governments have found it beneficial to convene all key stakeholders and participants to focus on creating and implementing a national initiative aimed at enhancing Internet safety for children and young people. This initiative also aims to increase awareness of relevant issues and provide practical solutions. It's essential to recognize that many individuals are consistently connected to the Internet through various devices. Therefore, broadband, mobile, and Wi-Fi operators should be actively engaged in this effort. Additionally, in numerous countries, public libraries, telecentres, and Internet cafes play a significant role in providing Internet access, especially for children and young people.
Research	7.	Conduct comprehensive research involving a wide range of national actors and stakeholders to assess their viewpoints, experiences, worries, and potential contributions regarding child online protection. This research should also gauge the degree of responsibility assumed by these entities, as well as their current or forthcoming initiatives aimed at safeguarding children in the online environment.	

Education digital literacy and competency	8.	Incorporate age-appropriate digital literacy components into the national educational curriculum, ensuring that they are suitable for all students.	Schools and the education system will serve as the cornerstone of the educational and digital literacy component within a national child online protection strategy. The national school curriculum should encompass child online protection elements, aiming to equip children of all age groups with age-appropriate skills to effectively utilize technology for their benefit while being aware of potential threats and risks to avoid. Furthermore, it should acknowledge and incentivize positive and constructive online behaviors. In any educational and awareness campaign, it's essential to strike the right balance. Messaging based on fear should be avoided, and emphasis should be placed on highlighting the numerous positive and enjoyable aspects of modern technology. The internet holds significant potential for empowering children and young individuals to explore new horizons. Teaching positive and responsible online conduct is a primary objective of education and awareness initiatives. Professionals working with children, particularly educators, should receive appropriate training and resources to effectively educate and impart these skills to children. They should possess an understanding of online threats and risks, along with the capability to confidently identify signs of abuse and harm, and take appropriate action to report and address these concerns to safeguard children.
Educational resources	9.	Leverage the insights and expertise of all stakeholders to create internet safety messages and resources that align with local cultural norms and legal frameworks. Ensure efficient distribution and appropriate delivery of these materials to all relevant target audiences. Explore collaboration with mass media to amplify awareness messages. Develop materials that highlight the positive and empowering aspects of the internet for children and youth while steering clear of fear-driven content. Promote constructive and responsible online conduct. Consider the creation of resources that assist parents in evaluating their children's online safety and educating them on strategies to mitigate risks and harness the potential benefits of the internet for their families through tailored educational initiatives.	When creating educational resources, consider that many individuals who are new to technology may not be at ease using it. Therefore, it's crucial to provide safety materials in written form or through alternative media formats that are more familiar and accessible to newcomers, such as video. Many major internet companies offer websites with extensive information on online issues for children and young people. However, frequently, this content is only available in English or a limited set of languages. Consequently, it's highly important to develop locally produced materials that align with both local laws and cultural norms. This local adaptation is essential for any internet safety campaign or training materials under development.

Child protection	10.	Establish comprehensive and consistent child protection procedures that require all professionals and institutions involved with children, including social services, healthcare providers, and schools, to recognize, address, and report instances of online abuse and harm.	There should be a standardized child protection system that applies to everyone involved in working with children, requiring them to report any cases of child abuse or harm to ensure proper investigation and resolution of such situations.
National awareness	11.	Conduct nationwide awareness campaigns to provide a platform for addressing child online protection issues on a universal scale. Utilizing global initiatives like Safer Internet Day could be advantageous in creating and promoting such campaigns.	Parents, guardians, and professionals, including educators, hold a vital role in ensuring the safety of children and adolescents in the online environment. It is essential to create supportive programs that not only raise awareness about online safety issues but also provide effective strategies for addressing them. Moreover, leveraging the mass media to promote awareness messages and campaigns should be considered. Utilizing opportunities like Safer Internet Day can effectively stimulate and facilitate a nationwide conversation on child online protection. Numerous countries have successfully organized national awareness campaigns centered around Safer Internet Day, involving a wide range of participants and stakeholders to disseminate a consistent message through various media and social platforms.
Tools, services, and settings	12.	Evaluate the significance of device configurations, technological resources (like filtering software), and child protection applications and adjustments that can be beneficial. Promote user accountability for their devices by endorsing operating system updates and the utilization of appropriate security software and applications.	There are various services accessible that can assist in filtering out undesirable content or preventing unwanted contacts. Some of these child safety and filtering programs may come at no extra cost as they are integrated into a computer's operating system or offered as part of a package by an ISP or ESP. Similarly, certain game console manufacturers provide similar tools for Internet-enabled devices. While these programs are not entirely foolproof, they can offer valuable support, especially for families with younger children. Most devices come equipped with settings designed to protect children and encourage balanced usage. These settings include features that allow parents to manage their children's devices, such as setting usage time limits, controlling which apps and services can be accessed, and overseeing purchases. Recently, reports and settings have been developed to help users and parents better monitor and regulate screen time and access. However, these technical tools should be viewed as just one part of a broader strategy. Parental or guardian involvement remains crucial. As children grow older, they will seek more privacy and independence. Additionally, in cases where a financial relationship exists between a vendor and customer, age verification processes can play a valuable role in reaching specific age-restricted audiences. However, in situations where no billing relationship exists, using age verification technology may be challenging, and in many countries, it may be infeasible due to a lack of reliable data sources.

EXAMPLE QUESTIONS

To gain a comprehensive understanding of the national landscape regarding online child protection, the following inquiries can be distributed among stakeholders and actors for their input. Their responses will play a crucial role in assessing policy coverage, identifying strengths, and pinpointing areas that demand special attention within a national checklist.

1. What is your level of responsibility concerning online safety and children's rights?
2. How have you integrated online safety and children's rights into your existing policies and operational procedures?
3. To what extent does existing legislation address online safety concerns?
4. What are your primary priorities related to online safety?
5. What initiatives and activities are you currently engaged in to promote online safety?
6. How do you collaborate with other agencies and organizations to enhance online safety?
7. Do you have mechanisms in place for children and parents to report online safety concerns or issues to you?
8. What are the three most significant challenges you face in the online realm?
9. What are the three most promising opportunities you see in the online environment?

Additionally, conducting research to understand the perceptions and experiences of children and their parents regarding online child protection would be valuable.

CONCLUSION

In today's digital age, the need to protect children online is paramount. Developing a National Child Online Protection Strategy is crucial for safeguarding the well-being and rights of children as they navigate the vast and complex online landscape.

This strategy encompasses various key areas of consideration. First and foremost, a robust legal framework must be in place, explicitly extending its reach to address online crimes against children. Laws should be adapted to the digital realm, criminalizing behaviors unique to the internet, such as grooming and remote enticement.

Regulation is another vital component. Whether through self-regulation, co-regulation, or comprehensive regulation, clear expectations and responsibilities must be established for all stakeholders. Reporting mechanisms for illegal content and user concerns should be easily accessible and widely publicized to ensure swift responses.

Collaboration among government agencies, law enforcement, social services, technology providers, educators, parents, and children is paramount. Research helps assess responsibilities and initiatives, while education equips children with digital literacy skills and promotes responsible online behavior.

Standardized child protection procedures are essential, requiring all professionals and institutions involved with children to recognize, address, and report online abuse and harm. Nationwide awareness campaigns amplify the message of online child protection.

Evaluating device configurations and promoting user accountability through security software and settings add critical layers to the strategy.

In conclusion, safeguarding children online is a shared responsibility that demands a holistic approach. A National Child Online Protection Strategy aims to create a safe, empowering, and educational digital environment for children, ensuring their rights and well-being are preserved as they explore the digital world.

ACKNOWLEDGEMENTS

These guidelines have been adapted from the ITU's Guidelines for Policy-makers 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 and policy-makers in addressing child online protection, valuable insights gleaned from various relevant reports and Focused Group Discussions (FGDs) conducted with policy-makers have been included.

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 Policy-makers 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 key Policy-makers in Bhutan. The localized guidelines were developed with the support from the International Telecommunication Union (ITU).