QUICK REFERENCE

CHILD ONLINE PROTECTION (COP) GUIDELINES FOR KEY STAKEHOLDERS: LOCALIZED FOR BHUTAN
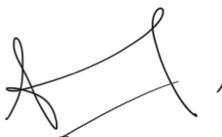
VERSION 1.0
2023

# FOREWORD

The Child Online Protection (COP) guidelines for Children, Parents & Educators, Policy Makers and Industry were released in 2020 by the International Telecommunication Union (ITU) capturing best practices and recommendations for various stakeholders to address the evolving digital landscape and new online safety challenges for children.

Bhutan's localized COP guidelines build upon the comprehensive framework of the original COP guidelines. Through background studies, assessments, and discussions, these guidelines incorporate Bhutan's specific context, including existing COP efforts and identified gaps. They also address the online risks faced by children and young individuals in Bhutan.

More than just highlighting online risks faced by Bhutanese children and young people, these localized COP guidelines provide a valuable resource with tailored recommendations for each stakeholder group. Parents and educators can find guidance on fostering safe online environments, while policymakers can leverage recommendations for strengthening COP mechanisms through collaboration with various stakeholders. The Industry guidelines equip companies with the knowledge to identify and prevent potential risks their products or services may pose to children's rights.

This particular document 'Quick Reference: Child Online Protection Guidelines for Stakeholders' provides the summary of recommendations for all the target groups acting as a quick reference for anyone or any agency who wants to look up the summary of the guidelines for all target groups. The link to the individual detailed guidelines can be accessed from www.tech.gov.bt/cop.

On behalf of the Govtech agency, I would like to thank the ITU for the generous support and guidance rendered to the COP working group in the development process. I would also like to acknowledge the efforts of the COP working group consisting of various stakeholders in the development of the guidelines. In addition I would like to thank UNICEF Bhutan for helping in planning and conducting the COP activities.

SECRETARY
GovTech Agency

QUICK REFERENCE


**CHILD ONLINE PROTECTION (COP) GUIDELINES FOR
KEY STAKEHOLDERS: LOCALIZED FOR BHUTAN**


GovTech Agency
Thimphu


**VERSION 1.0**
**2023**

# Table of Content

# INTRODUCTION

Two-thirds of the world's population have access to the Internet. The Internet penetration in Bhutan is relatively high - with around 94 percent of households and 86 percent of individuals with Internet connectivity.[1]  Mobile phones are the most common gateway and a lot of Bhutanese children reported accessing the Internet through phones. Worldwide, 75 percent of people aged between 15 and 24 years accessed the Internet in 2022, 10 percentage points more than among the rest of the population (65%).[2] In Bhutan, 93 percent of the students have Internet access at home, school, or community.[3]

At least four percent of Bhutanese students spend seven hours or more each day on digital devices and on the Internet; 34 percent of students spend between 1-2 hours; and around 30 percent spend less than an hour per day. Most students predominantly use mobile phones to access the Internet and 92 percent access the Internet at home [footnote 3]. Only about half of the students use the Internet at schools, local community facilities and Internet cafés. With increasing access and usage, the Internet has become integral to the lives of individuals, especially for children and youth.

Children go online for a variety of reasons such as learning, playing online games, social networking, and staying in touch with friends, among others. During the COVID-19 pandemic which resulted in school closure globally, most teaching and learning were conducted online. Children also use the Internet to search for information and learn online. Majority (81%) of Bhutanese students reported being competent in finding information to complete learning activities on the Internet (DKAP). While the Internet exposes children to boundless opportunities, it also exposes them to risks that may have a detrimental impact on their human rights, growth and development, and wellbeing.

DQ Institute notes that the world is experiencing a 'Cyber Pandemic' with around 60 percent of 8 - 12 years-old children online  exposed to cyber risk.[4] It is estimated that among children aged 8-12 years who use the Internet, 45 percent are affected by cyber-bullying;  39 percent are experiencing reputational risk; 29 percent are exposed to risky contents that are sexual and violent in nature; and 28 percent are experiencing cyber threats. Further, the children are exposed to cyber threats, and are at risk of gaming disorder and social media disorder.[5]

Almost eight in 10 children in Bhutan download or play games online irrespective of the area of residence. Around seven in 10 children like to watch or download photos, watch videos or listen to music online [footnote 1]. Children also reported experiencing online bullying, accessing inappropriate and risky contents online, and experienced identity theft resulting in reputational damage. In addition, insights from focus group discussions (FGDs) with various stakeholders revealed that students' online experiences were diverse. They derived enjoyment from popular games like Mobile Legends and PUBG and found value in the Internet for information, music, and entertainment. Nonetheless, they also encountered challenges like online bullying, exposure to inappropriate content, and instances of fake accounts and social media hacking. These findings underscore the critical need for fostering balanced and secure online engagement practices among students.

However, both parents and teachers shared that they lack awareness of the risk associated with children being online. Only 15 percent of households in the Information, Communications and Technology (ICT)

---

[1] MOIC, 2021, National ICT Household Survey, Nationwide ICT Household Survey Report.
[2] ITU, 2022, Measuring digital development: Fact and Figures. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx
[3] MOE, Digital Kids Asia Pacific, The Country Report Bhutan.
[4] DQInstitute, 2020, Child Online Safety Index, https://www.dqinstitute.org/wp-content/uploads/2020/02/2020COSIReport.pdf
[5] MToday,2020, Global study warns of 'cyber pandemic' among children; biggest risk for S'porean kids is cyber bullying, https://www. todayonline.com/singapore/global-study-warns-cyber-pandemic-among-children-biggest-risk-sporean-kids-cyberbullying

household survey are aware that their children are exposed to sexual content and around 13 percent of them know that their children face the risk of cyberbullying. Further, only around 10 percent of households are aware of the risk associated with online child grooming [footnote 1].

As most children learn to use the Internet and be online themselves, the risk of child online violence is high. For instance, owning a mobile phone increases the risk by 20 percent and highly active social media and gaming increases the risk by more than 40 percent [footnote 4]. Online safety of the children is critical to ensuring a high digital readiness that results in wise use of technology, respects family values, and future readiness with a positive career outline. On the other hand, an unsafe online environment will result in poor academic performance, mental health disorder and adverse long-term impact on individuals, family and society. Child online safety is a shared responsibility and requires concerted efforts of parents and guardians, school and educators, ICT service providers, and government and legislators.

## CHILD ONLINE PROTECTION

Recognizing the growing online risk and the need for a safe online environment for children and youth, International Telecommunication Union (ITU), a specialized agency of the United Nations, launched the Child Online Protection (COP) initiative in 2008[6]. COP aims to address the growing concerns about the risks and challenges that children and young individuals face when using the Internet and other digital technologies. The key feature of ITU's COP initiative are:

1. **Awareness and Capacity Building:** The initiative promotes a holistic approach to child online protection to build safe, gender-sensitive, age-appropriate, inclusive, and rights respecting digital environments for children and young people worldwide.

2. **Research and Knowledge:** Develops key recommendations and guidance to support all relevant stakeholders in their efforts to create a safe and empowering online environment for children and young people allowing them to realize the full range of their rights.

3. **Global Programming and International Cooperation:** Supports Member States in drafting, adoption and implementation of COP National Frameworks and comprehensive strategies that involve all relevant stakeholder groups. The initiative also facilitates international collaboration and cooperation among governments, industry stakeholders, and civil society organizations to address global online safety challenges.[7]

Bhutan became a member of ITU in 1988[8] and participates in international telecommunications and ICT standardization, regulation, and cooperation efforts, contributing to the global development and governance of telecommunications and ICT networks and services. To enable Bhutan to build an ICT-enabled knowledge society, the government established Bhutan Computer Incident Response Team (BtCIRT) to ensure secure and reliable ICT services in 2016[9].

Recognizing the national risk resulting from increasing violence and risk to children and youth online, BtCIRT partnered with ITU, and UNICEF Bhutan to develop and adopt COP guidelines for Bhutan.

[6] ITU, 2020 Child Online Protection, Https://www.itu.int/en/cop/pages/default.aspx.
[7] ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx
[8] Ministry of Foreign Affair and External Trade, List of UN, related organizations, intergovernmental organizations of which Bhutan is a member.https://www.mfa.gov.bt/list-of-un-related-organizations-intergovernmental-organizations-of-which-bhutan-is-a-member/
[9] BtCIRT. https://www.btcirt.bt/about-us/

The current guideline is a result of collaborative efforts between ITU, Unicef, GovTech and different stakeholders including law enforcement, regulators, child protection and education agencies, multilateral partners, Civil Society Organizations (CSOs), among many others.

## WHO IS THIS GUIDELINE FOR?

This short guideline is a summary of COP guidelines for children, educators and parents, industry and policy-makers. This is intended to be primarily used by parents and educators and longer versions of the guidelines for children with age-appropriate materials and language, and guidelines for educators and parents are publicly available. While primarily intended for parents and educators, the guidelines also cover the roles of industry and policy-makers in brief. The guideline is organized into different sections for different stakeholders and provides generic roles and guidelines to ensure a safe online environment for children and youth. The last section provides links and contacts to agencies where stakeholders may report in the event of violence against children online or if any individual come across child sexual abuse materials (CSAM).

## GUIDELINE FOR CHILDREN

All children and young people around the world have the right to a safe experience online. The COP Initiative has identified three principal age groups of children corresponding to key stages of child's development. The three age groups are:

1. **5 - 7 years old:** This group experiences their first contacts with technology. Their access and activities on the device and the Internet should be closely supervised at all times by a parent or adult. This age group may not be able to comprehend complex ideas, content and messages. Parents or adults with responsibility for children should consult the COP guidelines for parents, guardians and educators to see how they might best assist their children stay safe online.

   a. **Right to play online:** All children have the right to play as enshrined under Article 31 of the Convention on the Rights of the Child (CRC). This could include playing games, watching videos, and connecting with friends and family online, as appropriate for their age.

   b. **Managing screen time:** It is important for a child's health and wellbeing that their screen time is balanced with offline activities. Fun offline activities could include imaginative play inside or outside, reading books, doing art and playing sports.

   c. **Exposure to inappropriate content:** Sometimes children are accidentally exposed online which are inappropriate, scary, upsetting or rude. It is important that children know they can always talk to a trusted adult about what they saw, how it affects them, and what they can do when these things happen.

   d. **Right to use digital media to learn:** In line with the rights enshrined in article 13 and 17 of the CRC, all children have the right to access information, to learn and to develop new skills. Digital media can support these things. For example, there are many educational websites built just for children.

   e. **Privacy:** Keeping personal information, including photos, and any other information that reveals their identity must be protected and their right to privacy be observed at all times to keep children safe online as well as offline.  Many websites and apps have privacy settings to help keep information private.

2. **8 - 12 years old:** This age span is considered a challenging transition as this stage is marked by curiosity. Their curiosity may push them to seek out and challenge boundaries, looking for their own answers. Their uncritical approach to content and contact may create a vulnerable situation which may be exploited by predators and commercial entities wishing to engage with them. Therefore, parental supervision and teachers' engagement at this age is critical to ensure that they are safe online.

   a. **Understanding right vs want:** A child has the right to health, education, family life, play and recreation and adequate standard of living and to be protected from abuse and harm. Every child must be able to recognize their rights to be protected both online and offline without discrimination in all forms as well as give due weight to their views in any decisions that affect children.

   b. **Sharing online:** Online activities such as social media posts, personal information, location and search history can be seen by friends and family, businesses, government, strangers and tech companies. A child needs to understand who can view what they have shared and who have access to their online activities.

   c. **Trust:** Trusting information on the web can be challenging because the Internet is a vast and open platform where anyone can publish information and content. Children need to learn strategies to evaluate and determine the trustworthiness of information and contents.

   d. **Messaging:** Children message with friends a lot and it is important that they learn how to safely message with friends, family and strangers.

   e. **Blocking:** Blocking can be an effective way to stay safe online and children should learn what kind of messages or contacts to be blocked. Children need to learn to block harassment, cyberbullying, spam and scams, inappropriate contents and unwanted contacts.

   f. **Reporting and support:** When children encounter violence online or come across inappropriate contents, they need to know where to report and seek support.

   g. **Shield:** Viruses and malware can slow down computers or crash, or they can delete files or even put your privacy or security at risk. Children need to learn how to protect their computer and devices and sites that they should avoid.

3. **13 years old and above:** This group experiences rapid growth, transitioning from being young people to becoming young adults. In this age group, they explore and develop their own identities, and their own tastes. Children in this age group are able to use technology with a high level of proficiency, without any adult support, supervision or interaction. Their hormonal development and a growing sense of physical maturity may lead them to find their own way to escape parental or adult supervision and seek out their peers. Their natural curiosity about sexual matters may put them in potentially worrying situations. The risk makes it important for all children, particularly this group to understand how to stay safe online. The following are the guidelines for children of this age group:

   a. **Rights:** All children, whether they are online or offline are protected by legal rights particularly in the spirit of the Constitution of the Kingdom of Bhutan and the CRC. Children have the right to be protected from harm, privacy, access and use technology, express opinion freely, health, family environment, justice, play and recreation, be informed and be educated around the principles of right to non-discrimination, participation, protection and best interest of the child.

b. **Privacy:** Children have rights to keep their personal information private and protect their identity. Children should learn how to use the internet for personal development as well as protect from harmful effects such as securing their password and personal information.

c. **Trust:** Children should learn that not everything that they see online is true and authentic. Children should authenticate the information that they see online and seek support of parents, teachers and other stakeholders in validating the information.

d. **Be Kind:** Every child has the right to be treated with respect online. It is unacceptable for anyone including children to be disrespectful online to others.

e. **Trolls:** Every child should be protected from upsetting and offensive contents online. Children need to learn ways such as blocking, sharing information with someone whom they trust, and ignoring inappropriate contents to be safe online.

f. **Have Boundaries:** Every child should be protected from sexual exploitation and other forms of violence. They should learn to say NO and set boundaries online to protect themselves from sexual exploitation, harassment and other forms of abuse online.

g. **Meeting People:** Young people make a lot of friends online and often they want to meet their online friends in person. Children should inform their parents about their meeting, and should always avoid meeting during odd times and places.

h. **Balance:** Most people spend significant time on the screen. It is important to monitor screen time and ensure that there is balance time allocated with offline activities.

## GUIDELINES FOR PARENTS, CARERS, AND GUARDIANS

The guideline stresses the need for parents to support their children in using technology safely, balancing the educational and social benefits of the Internet. Safety tips are provided based on research to guide parents in ensuring a positive online experience. Parents should assess websites, understand their children's online risks, and their own ability to mitigate these risks. It underscores the Internet's potential to empower children and emphasizes the importance of teaching responsible online behavior.

1. **Open Dialogue and Shared Online Activities:** Ongoing communication with children about online activities is vital. Parents should engage in online activities with their children to build trust and understanding. Fostering open communication encourages children to discuss online issues. Stakeholders from the FGDs stress that parents should proactively set boundaries and maintain open communication to ensure their children's online well-being. This proactive approach builds trust and helps address online concerns effectively.

2. **Identify Technology and Services:** Maintaining a comprehensive list and understanding of all family-connected devices and online services, including mobile devices, gaming consoles, and apps, is crucial. However, focus group findings reveal that this is a widespread issue, particularly in Bhutan, where parents often lack awareness due to their busy schedules or literacy. In some cases, they pass gadgets to their children without understanding their online activities, emphasizing the urgent need for greater parental involvement and digital awareness to ensure children's online safety.

3. **Device Security:** For online safety, parents must engage actively by securing devices with firewalls, antivirus software, and updates. Open discussions about privacy and responsible online behavior are vital. FGD findings stress parental involvement due to online risks, especially for children lacking knowledge and skills on security measures. Parents should also be aware of laws on collecting personal information and check service requirements for parental consent, ensuring compliance, especially for younger children.

4. **Establish Family Rules and Expectations:** Setting clear family guidelines for Internet and device use is vital, addressing privacy, content, bullying, screen time, and online interactions. It's essential to foster a supportive and conducive environment where children feel safe seeking help or support. Stakeholders in FGDs noted that rules can also prevent device addiction and strain on family relationships, emphasizing the importance of establishing these guidelines in a positive and constructive manner.

5. **Awareness of Children's Online Activities:** Lack of awareness among parents regarding their children's online activities is a prevalent issue. It's imperative for parents to stay informed about the online services, apps, and games their children use. Understanding how to promote safe usage, like setting accounts to private and adhering to age restrictions, is crucial. As FGDs suggest, parents can further enhance awareness by utilizing parental control tools and engaging in open discussions about their children's online motivations and experiences.

6. **Know How to Report and Control Content:** Parents must understand how to report issues on the platforms their children use, including the knowledge of deleting or modifying profiles when necessary. Additionally, awareness of local reporting helplines is crucial to effectively address concerns. Unfortunately, the lack of parental knowledge about these reporting resources is further compounded by children not sharing their online issues and threats with their parents, underscoring the need for open communication and education on these matters.

7. **Address Advertising and Misinformation:** Discussing inappropriate or misleading ads is important. Encourage children to report them and promote online media literacy. Emphasize that the online world reflects both positive and negative experiences, fostering open communication for support. Teach children to recognize risks like coercion and blackmail, stressing responsible online behavior in line with prevailing laws and policies

8. **Meeting Online Contacts in Real Life:** According to the FGD participants, numerous instances of online child grooming leading to in-person meetings were recounted, highlighting the pressing need to educate children about the risks involved in meeting online contacts in person. It is imperative that parents take an active role in this regard, offering to accompany their children or arranging for a trusted adult to be present when such meetings are considered to ensure the safety and well-being.

9. **Protecting Personal Information:** Many children have firsthand experience with the issues that arise from sharing personal information and photos, especially on social media. Therefore, it is critical to teach children how to protect their online personal information. Emphasize the importance of not sharing identifiable details and highlight the risks associated with posting revealing photos. Encourage a consent-based approach to photo sharing to enhance online safety and help children navigate the digital world more responsibly[10].

---

[10] ITU Publications, 2020, Guidelines for parents and educators on Child Online Protection. http://handle.itu.int/11.1002/pub/8158f72a-en

# GUIDELINE FOR EDUCATORS

Educators also play a vital role in safeguarding children and young people online, whether in formal or informal learning settings. While some responsibilities, such as filtering and monitoring, may be beyond their control and are typically implemented at the school or institution level, educators can still contribute significantly to a safe and positive online experience for their students.

1. **Device Security and Passwords:** Device security is vital in education, as highlighted in the FGD findings. This entails strong passwords, device lockdown when idle, and regular antivirus/ firewall updates. Schools should create age-appropriate Acceptable Use Policies (AUP) and designate an Online Safety Coordinator, engaging school management and stakeholders for enforcement. Collaboration with accredited ISPs enhances network security. Filtering and monitoring tools restrict inappropriate content access, enhancing student safety in the digital learning environment.

2. **Adherence to School Policies:** The shift to digital education, accelerated by COVID-19, has reshaped school policies. Schools must adapt to technology's evolving nature, particularly students' personal device use. Safety in this dynamic digital landscape necessitates ongoing education and open discussions. Educators and students must adhere to technology-related school policies, setting examples and following guidelines for mobile device use to uphold an effective learning environment.

3. **Training and Awareness:** FGD findings highlight a significant gap in Bhutanese educators' readiness to address online threats. To create an environment where students feel comfortable sharing concerns, comprehensive online safety training is essential for all staff, including support personnel. This training should cover technical aspects and educate staff on the educational and psychological effects of the Internet and online technologies on students, enabling educators to better assist students in navigating the digital landscape.

4. **Images of Pupils:** Respecting school policies regarding the taking of photographs of students is crucial. Obtaining necessary permissions from parents, caregivers, or students for any photography is a fundamental aspect of maintaining privacy and consent. Encouraging the use of school-approved devices for educational photography helps ensure that these practices align with school guidelines.

5. **Filtering and Monitoring:** Respecting school policies on photographing students is vital. Obtaining permissions from parents or students for photography ensures privacy and consent. The use of school-approved devices for educational photography aligns with guidelines. As discussed in FGDs, sharing student photographs with personal information can make students vulnerable to online threats, underscoring the need for careful handling of such data. It is also important to incorporate such aspects in school policies.

6. **Online Reputation and Digital Footprint:** To protect personal and school reputations, it is crucial to maintain a professional online presence. Educators should teach students how to manage their online reputations effectively, emphasizing professionalism in online interactions to avoid potential pitfalls.

7. **Professional Online Communication:** Clear boundaries should be maintained between personal and professional online activities. Using a school email address for communication with

students, parents, and stakeholders is advisable. Additionally, one-on-one digital communication and the use of personal devices for such purposes should be minimized. Clear expectations for video-conferencing and remote learning should also be set.

8. **Non-Formal Settings and Support:** In addition to formal classrooms, extending online safety awareness to non-formal settings, such as youth clubs, is crucial. During FGDs, the formation of clubs and youth support groups was recommended, as children tend to feel more comfortable sharing with peers of their age group rather than adults. Educator facilitation can play a pivotal role in fostering these safe and supportive spaces for discussions and learning about online safety among young people.

9. **Incident Reporting and Auditing:** Schools should create a central reporting point where online safety incidents can be documented and analyzed for insights into emerging issues. Regular audits of safety measures should be conducted to assess their effectiveness and make necessary improvements.

10. **Understanding Online Risks and Benefits:** Educators should be well-acquainted with the online activities of children and young people. They should strive to understand the potential risks and benefits that students may encounter when they navigate the online world, allowing them to provide guidance and support that ensures safe and responsible Internet usage [footnote 10].

## GENERAL GUIDELINES FOR INDUSTRY

The role of industry in COP is significant and encompasses various responsibilities, actions, and initiatives to ensure the safety and well-being of children while they engage with digital technologies and online platforms. The guidelines in this document outline broad recommendations for industry for identifying, preventing and mitigating any adverse impacts of products and services on children and young people's rights, and for promoting children and young people's positive use of ICTs.

1. **Development of policy:** Industry can identify, prevent and mitigate the adverse impacts of ICTs on children and young people's rights, and identify opportunities to support the advancement of children and young people's rights. This can be done by developing a child protection and safeguarding policy and/or integrating specific risks and opportunities pertaining to children and young people's rights into company-wide policy commitments.

2. **Engaging with other stakeholders:** In collaboration with government, law enforcement, civil society and other related organizations, industry has a key role to play in combating Child Sexual Abuse Material (CSAM). Companies can prohibit uploading, posting, transmitting, sharing or making available content that violates the rights of any party; communicate with law enforcement agencies or other organizations to report SCAM at the earliest; and ensure that internal procedures are in place to comply with reporting responsibilities.

3. **Enhancing the digital experience:** Industry can help create a safer, more enjoyable digital environment for children and young people by adopting safety and privacy-by-design principles in the company's technologies and services, implementing age-appropriate designs, among others.

4. **Incorporate educational and empowerment initiatives:** Complement technical measures with educational and empowerment activities by educating customers, collaborating with schools and government to educate parents, and by providing educational materials to schools and religious institutions such as in monasteries and nunneries.

5. **Leveraging the use of Artificial Intelligence:** Industry can use technology to protect and educate children such as use of privacy-preserving AI to protect children online.

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

## GENERAL GUIDELINES FOR POLICY-MAKERS

Policy-makers[11] hold crucial responsibilities considering the rapid evolution of technology. The conventional approaches to policy making are now inadequate for the task at hand. To effectively protect children in the dynamic digital age, policy-makers must construct a legal framework that is not only adaptive and inclusive but also finely tailored to the swiftly changing technological landscape. The objective of these guidelines is to furnish policy-makers with a user-friendly and adaptable framework, enabling them to comprehend and fulfill their legal duty to ensure the safety of children in both real, physical and virtual worlds.

These guidelines, grounded in research and existing models, provide clear recommendations for crafting a national child online protection strategy. In this process, policy-makers must consider various facets:

1. **Engaging with stakeholders:** To gain insights into experiences, perceptions, opinions, and ongoing initiatives, they should first identify and collaborate with a diverse range of stakeholders, including children and young people, parents, guardians, educators, government ministries, industry and connectivity providers, research and academia, non-governmental organizations, law enforcement, and health and social services.

2. **Acknowledging existing activities:** It's quite likely that numerous stakeholders have independently initiated efforts to protect children online, albeit in isolation. To develop an effective national child online protection strategy, it's imperative to acknowledge and appreciate these pre-existing activities. The strategy should aim to coordinate and streamline both existing and new activities, seamlessly integrating into or referencing existing national frameworks or strategic plans. This cohesive approach ensures a well-rounded and comprehensive approach to safeguarding children in the online world.

3. **Benefit towards protection of children:** A national strategy for safeguarding children on the Internet offers evident advantages. The establishment of suitable national laws, the corresponding legal structure, and, within this strategy, alignment on the global stage, play crucial roles in ensuring the online protection of children. These frameworks can take the form of self-regulation, co-regulation, or full regulatory mechanisms.

---

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

4. **Establishment of a multi-stakeholder mechanism:** A multi-stakeholder mechanism needs to be created to delineate, coordinate, and propel the initiatives outlined in the national child online protection strategy. This mechanism should serve as the means to convene and harmonize the diverse array of national participants and stakeholders involved in these efforts.

## WHERE TO GO FOR HELP?

Child safety is a paramount concern in Bhutan, and robust measures have been instituted to protect children online. Reporting and support mechanisms are available at international and national level. At the national level, the following helplines are available:

1. **1098** is a toll-free helpline for women and children handled by The PEMA Secretariat for those in need of support and services. Anyone can call the hotline and report both offline and online violence against children. NCWC mobile app for android and iOS is available under the G2C Bhutan Apps for reporting, support and education.

2. **1010/112** is a helpline service provided by The PEMA Secretariat for all mental health related support. The PEMA Helpline provides information, online counseling as well as referral and linkages.

3. **113** is toll free managed by Royal Bhutan Police (RBP) for reporting crime in Bhutan. Further, support can be sought by making walk-in complaints to the Women and Children Unit or Desk of RBP.

4. **BtCIRT** is mandated to enhance cyber security in Bhutan and accepts anonymous incident reports. Reports can be filed to BtCIRT at cirt@btcirt.bt

5. **1257** provides youth outreach by Nozhoen Lamtoen[12]1600 and 7700 are helplines for Bhutan Telecom and TashiCell. Complaints and reports can be filed against individuals or contents to the service providers.

At the international level, reports can be filed to following website:

1. **Internet Watch Foundation (IWF)** helps victims of child sexual abuse worldwide by identifying and removing online images and videos of their abuse. The foundation accepts anonymous reports and each report is processed manually by highly trained analysts. You can report any CSAM to IWF at https://www.iwf.org.uk/report/

2. **Child Helpline International** publishes and provides links to child helplines in every country. It also provides help, support and counseling services to children (18 years and under) and/or young people (25 years and under) through online and offline means of communication. https://childhelplineinternational.org/

---

[12] CSOA, Nozhoen Lamtoen. http://www.csoa.org.bt/public/pbinfo/contacttrustee/27

Many social media companies have embedded reporting mechanisms into their platforms. The following links provides help and process of reporting in few of the popular platforms:

1. Facebook: https://www.facebook.com/help/reportlinks
2. Google: https://support.google.com/families/answer/7182800?hl=en
3. Roblox: https://en.help.roblox.com/hc/en-us/sections/200866000-Safety
4. Instagram: https://help.instagram.com/192435014247952
5. Tiktok: https://www.tiktok.com/safety/en/prevent-csam/
6. Snapchat: https://values.snap.com/safety/safety-reporting

The detailed COP guidelines for the various targets can be found in www.tech.gov.bt/cop

## ACKNOWLEDGEMENTS

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

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

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

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

9. Department of School Education (DSE), Ministry of Education and Skills Development

10. Bhutan Telecom Ltd.

11. Tashi Cell

12. The former Ministry of Information & Communications

13. The former Department of Information and Media

# DISCLAIMER



**Australian Government**

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