







GUIDELINES FOR PARENTS AND EDUCATORS ON CHILD ONLINE PROTECTION (LOCALIZED FOR BHUTAN)

VERSION 1.0 2023

ON CHILD ONLINE PROTECTION (LOCALIZED FOR BHUTAN)

	Executive Summary	1
	Introduction	2
	What is child online protection?	5
	Children and young people in a connected world	5
	A world of fun	7
	Making new connections	7
	The joy of creation	8
	An appetite for information	8
	Becoming active citizens	9
	Running risks and suffering harm	10
	Privacy is a priority	11
	Home is where the Wi-Fi is	12
	Children with vulnerabilities	13
	Migrant children	13
	Children with Autism Spectrum Disorder (ASD)	14
	Children with disabilities	14
	New and emerging risks and challenges	15
	Internet of Things	15
1.1	Connected toys and robotics	16
	Online Gaming	18
	Artificial intelligence and machine learning	20
	Understanding risks and harms	21
	Online manipulation	21
	Online solicitation or grooming	22
1.1.1	Bullying and harassment.	22
	Sexting	24
	The role of parents, carers and guardians can play	25
	Where to go for help?	27
	Guidelines for parents, carers and guardians	28
	The role of educators	32
	Informal education settings	35
	Managing devices, filtering, and communication	35
	Training and support	35
	Guidelines for educators	36
	Conclusion	38
	CONTOURS	50

EXECUTIVE SUMMARY

In an increasingly digital world, children and young people are exposed to various online risks. Sexting and the creation of illegal child sexual abuse material are serious concerns, leading to potential legal consequences. Additionally, issues like health risks related to excessive screen time, copyright infringement, misrepresentation of age, and unauthorized use of parental email accounts pose threats to young individuals' online safety.

Efforts to promote online safety should be a collective endeavor, involving parents, caregivers, educators, and other stakeholders. Online safety campaigns aim to change behavior, encourage safer online practices, effective parenting, and responsible interactions with children and young people in digital environments.

Parents and guardians play a crucial role in supporting children's safe online experiences. They should be aware of potential online risks and actively engage in their children's digital activities. Open and age-appropriate dialogues about online risks, critical thinking, peer pressure, addictive technologies, and balanced digital use are essential for fostering a safe online environment.

Educators, too, have significant responsibilities in promoting online safety. They must teach children about online risks, privacy protection, and responsible online behavior. Digital citizenship education should be integrated into curricula, focusing on social and emotional learning to develop healthy online relationships.

Schools should establish robust online safety policies, acceptable use policies (AUP), and anti-bullying policies. An online safety coordinator can oversee these efforts. Infrastructure, secure networks, filtering, and monitoring tools should be in place to safeguard students.

Children often access the Internet in various settings, including informal ones like youth clubs. Educators and support staff in these environments should also be equipped to understand online risks, manage personal devices, and address the use of mainstream social media and messaging services.

Ultimately, comprehensive online safety involves a coordinated effort among parents, educators, caregivers, and other stakeholders. By actively engaging in children's online experiences, teaching responsible digital citizenship, and establishing robust policies and practices, we can create a safer digital world for the younger generation.

INTRODUCTION

In 2022, around two-thirds of the world's population was using the Internet, Approximately two-thirds of the population in the Arab States and Asia-Pacific countries (70 and 64 percent respectively) use the Internet, in line with the global average, while the average for Africa is just 40 per cent of the population. Worldwide, 75 percent of people aged between 15 and 24 use the Internet in 2022, 10 percentage points more than among the rest of the population (65 per cent)¹. In 2019, globally, one in three Internet users was a child (0-18 years old), with approximately 71 percent of young people already being online according to UNICEF estimates². In 2021, an estimated 94.3 percent of households in Bhutan had Internet access. In 2020, around 68 percent of students reported accessing the Internet, with 34 percent spending 1-2 hours on digital devices daily, 30 percent spending less than an hour, and four percent spending seven hours or more. The widespread availability of Internet access points, mobile technology, and a growing range of Internet-enabled devices, coupled with the vast resources in the digital realm, offer unprecedented opportunities for learning, sharing, and communication³.

With more children around the world gaining access, the fulfilment of their rights will increasingly be shaped by what happens online. Internet access is fundamental to the realization of children's rights. In terms of access to the Internet, there are also significant differences by gender. Research shows that in every region except the Americas, male Internet users outnumber female users. In many countries, girls do not have the same access opportunities as boys, and even where they do, girls are often monitored and restricted in their Internet use to a much greater extent. On a global scale, 69 per cent of men are using the Internet, compared with 63 percent of women. This means there are 259 million more men than women using the Internet in 2022⁴. Bhutan is committed to gender equality, ensuring that both males and females have equal access to the internet and modern technologies. The government's Gross National Happiness philosophy emphasizes well-being and social inclusion, with initiatives aimed at bridging the digital gender gap through internet access and technology training. While challenges may exist in specific areas, Bhutan's ongoing efforts prioritize equal opportunities, including in the realm of technology and the Internet.

As more children across the globe gain internet access, the realization of their rights increasingly depends on their online experiences. Access to the internet is a fundamental component of children's rights, but gender disparities persist, with research indicating that, except in the Americas, male internet users outnumber females. In many countries, girls face unequal access opportunities and greater restrictions on their internet use⁵. Globally, 69 percent of men use the internet compared to 63 percent of women, resulting in 259 million more male internet users in 2022. Bhutan is dedicated to gender equality, promoting equal access to the internet and technology for both genders, aligned with their Gross National Happiness philosophy focusing on well-being and social inclusion. Bhutan's initiatives aim to bridge the digital gender gap by providing internet access and technology training, prioritizing equal opportunities in the technological realm, and reflecting their commitment to equal rights.

Digital divides go beyond the question of access. Children who rely on mobile phones rather than computers may get only a second-best online experience, and those who lack digital skills or speak minority languages often cannot find relevant content online. Children from rural areas are more likely to experience theft of passwords or money. They also tend to have lower digital skills, spend more

ITU (2022), Measuring digital development: Fact and Figures. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

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

³ MOIC, (2021), National ICT Household Survey, Nationwide ICT Household Survey Report.

⁴ ITU, 2022, Measuring digital development: Fact and Figures. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

⁵ Araba Sey and Nancy Hafkin, 2019, REPORT OF EQUALS RESEARCH GROUP, LED BY THE UNITED NATIONS UNIVERSITY. https://i.unu.edu/media/cs.unu

time online (especially playing games), and receive less parental mediation and monitoring⁶.

The Internet has become a tremendously enriching and empowering technology. Children and young people have been major beneficiaries of the Internet and related digital technologies. These technologies are transforming how we communicate and have opened many new ways to play games, enjoy music and engage in a vast array of cultural activities and participation, dissolving many barriers. Children can broaden their horizons online, by taking advantage of opportunities to gather information and nurture relationships. Access to ICTs offers children literacy skills that further other forms of participation offline.

The Internet provides access to health, educational services, and information on topics that are important for young people but may be taboo in their societies. Children and young people have very often been at the forefront of adopting and adapting to the possibilities provided by the Internet.

Yet, it is undeniable that the Internet has brought in its wake a range of challenges to children's and young people's safety, which need to be addressed, both because they are important in their own right but also because it is important to communicate to everyone concerned that the Internet is a medium that can be trusted. Equally, it is essential that the concern to protect children and young people online is not allowed to become a platform to justify an assault on free speech, free expression or the freedom of association.

It is extremely important for the next generation to feel confident about using the Internet in order that they can, in turn, continue to benefit from its development. Thus, when discussing children's and young people's safety online, it is vital to strike the right balance.

It is essential to openly discuss the risks that exist for children and young people online, to teach them how to recognise risk, and prevent or deal with harm should they materialize, without unduly frightening or exaggerating the dangers.

Any approach that deals only or largely with the negative aspects of technology is very unlikely to be taken seriously by children and young people. Parents and teachers can often find themselves at a disadvantage because young people will very often know more about technology and its possibilities than older generations. Research has shown that the majority of children are able to distinguish cyberbullying from joking or teasing online, recognising that cyberbullying is designed to harm. In many parts of the world, children indeed understand some of the risks they face online⁷. While young people and students in Bhutan may have some awareness of internet risks and cyberbullying, there may be a gap in their knowledge compared to children in more developed and technologically advanced countries. This difference in awareness can be attributed to variations in access to digital education, cybersecurity awareness programs, and the level of internet penetration and exposure to online platforms.

However, while it might be deduced that efforts to skill children to manage online risks are effective, there is still scope to raise the awareness of many more children around the world, particularly among vulnerable groups, and concerted efforts must focus on these children, especially to improve awareness of support services for victims of cyberbullying and other forms of online risks. In the digital age, ensuring the safety and well-being of children online has become a paramount concern for societies worldwide, including Bhutan. With the rapid expansion of internet access and digital technologies,

⁶ UNICEF, 2019, Growing up in a connected world. UNICEF Office of Research-Innocenti, Florence. https://%20www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf

⁷ Since 2016, ITU undertakes consultations within COP with children and adult stakeholders on relevant issues such as cyberbullying, digital literacy and children's activities online.

Bhutanese children are increasingly engaging with online platforms, creating new opportunities and challenges. The Royal Government of Bhutan, along with various stakeholders, recognizes the need for comprehensive child online protection measures to safeguard children from potential risks such as cyberbullying, inappropriate content, and online exploitation⁸.

There are many challenges ahead. Not only does access to the connected world pose problems. The rate of technological change presents challenges for the safety of children online. Many children navigate a complex digital media landscape. Developments in artificial intelligence and machine learning, virtual and augmented reality, big data, facial recognition, robotics and the Internet of Things are set to transform children's media practices even further.

It is critical that all stakeholders plan for and think through the consequences of these developments for children and find ways to support them to develop the necessary digital literacies not just to survive but to thrive in the digital future. Further investment in the digital skills and literacies of parents and teachers is required to support children to develop the critical thinking and evaluative skills to enable them to navigate fast-paced flows of information of varying quality, and from parents and educators to children, to become digital citizens⁹.

Recognizing the profound impact of the digital age on today's youth, the discussions emphasized the essential roles parents and educators play in guiding children's interactions, learning, and safety in the online world. As children grow up with the internet as an integral part of their lives, parents are urged to actively engage with their children, fostering open dialogues about online risks, responsible behaviour, and the importance of digital literacy. Meanwhile, educators are encouraged to incorporate comprehensive strategies into their curricula that promote safe and ethical online practices, equipping students with the skills needed to navigate the digital landscape securely. The minutes underscore the collaborative efforts required to create a nurturing environment that empowers children and young people to harness the benefits of the Internet while minimizing potential risks.

Balancing children's online opportunities and risks remains a challenge. The ITU Member States also indicated that while efforts to promote opportunities for children online must continue to be a priority, this must be carefully balanced with rights to safe conditions under which they can participate in and benefit from the digital world¹⁰.

ITU's COP Initiative outlines comprehensive guidelines that encompass all relevant stakeholders, including Bhutanese children and young people. These guidelines serve as a comprehensive framework to ensure online safety and empower individuals to protect themselves and others while navigating the digital realm. They offer a blueprint that can be tailored to align with Bhutan's unique cultural norms and legal framework.

Within the context of Bhutan, this report has been developed through collaboration between the ITU's COP Initiative and Bhutanese experts. This multi-stakeholder approach leverages inputs from various sectors and perspectives within Bhutan to provide invaluable insights. The report's primary focus is to offer informative content, practical advice, and safety recommendations specifically tailored for parents, guardians, and educators in Bhutan. By combining international expertise with Bhutan's local context, the report contributes to the goal of cultivating a safer online environment for the country's children and young people.

⁸ MoIC Royal Government of Bhutan (2021), National Information Communications Technology (ICT) Policy.

⁹ Council of Europe (2016), Digital Citizenship Education. https://www.coe.int/en/web/digital-citizenship-education/home

¹⁰ ITU News (2018), Celebrating 10 Years of Child Online Protection. https://news.itu.int/celebrating-10-years-child-online-protection/

WHAT IS CHILD ONLINE PROTECTION?

Online technologies offer many possibilities for children and young people to communicate, learn new skills, be creative and contribute to establishing a better society. But they can also bring new risks such as exposing them to issues of privacy, illegal content, harassment, cyberbullying, misuse of personal data, grooming and even child sexual abuse.

These guidelines develop a holistic approach to responding to all potential threats and harms that children and young people may encounter when acquiring digital literacy. They recognise that all relevant stakeholders have a role in their digital resilience, well-being, and protection while benefiting from the opportunities that the Internet can offer.

Protecting children is a common responsibility and it is up to all relevant stakeholders to ensure a sustainable future for all. For that to happen, policy-makers, the private sector, parents, carers, educators and other stakeholders, must ensure that children can fulfil their potential – online and offline.

Crucially, parents and educators share significant responsibilities in the realm of COP. Parents play a pivotal role in guiding their children's online experiences. By staying informed about the digital platforms their children use, setting guidelines, and promoting open communication, parents can create an environment where children feel comfortable discussing any online concerns they encounter¹¹. Equipping children with critical thinking skills to discern trustworthy information from misinformation is equally vital.

Educators, too, play a vital role in COP. They can incorporate digital literacy and online safety education into their curricula, helping students develop the skills to navigate the internet responsibly. Educators can facilitate discussions on digital ethics, respect, and empathy, fostering a culture of responsible online behavior. By identifying signs of distress related to online experiences, educators can provide timely support and guidance to affected students¹². In recent years, mobile Internet access has increased tremendously and there is no silver bullet solution to protect children and young people online. This is a global issue that requires a global response from all sectors of society, including children and young people themselves.

In order to respond to these growing challenges in the face of the rapid development of ICTs, the Child Online Protection (COP) Initiative ¹³, a multi-stakeholder international initiative launched by ITU in November 2008, continues to bring partners together from all sectors of the global community to create a safe and empowering online experience for children and young people around the world. It sets out guidelines for all relevant stakeholders including children and young people in all parts of the world on how to keep themselves and others safe online. These guidelines act as a blueprint, which can be adapted and used in a way that is consistent with national or local customs and laws.

CHILDREN AND YOUNG PEOPLE IN A CONNECTED WORLD

In 2022, around two-thirds of the world's population was using the Internet, Approximately two-thirds of the population in the Arab States and Asia-Pacific countries (70 and 64 percent respectively) use the Internet, in line with the global average, while the average for Africa is just 40 per cent of the

¹¹ UNICEF (2019), Child online protection: Guidelines for industry, https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf

¹² European Commission (2020), Better internet for kids: Guide to online safety for children, https://digital-strategy.ec.europa.eu/en/policies/better-internet-kids

¹³ ITU (2020), Child Online Protection, Https://www.itu.int/en/cop/pages/default.aspx.

population. Worldwide, 75 percent of people aged between 15 and 24 use the Internet in 2022, 10 percentage points more than the rest of the population (65 per cent)¹⁴. In 2019, globally, one in three Internet users was a child (0-18 years old), with approximately 71 percent of young people already being online according to UNICEF estimates¹⁵. The FGD conducted with Bhutanese students in the ITU consultation, a clear observation emerged: the present generation of children in Bhutan is maturing alongside the internet, which has seamlessly integrated itself into their daily lives. This integration has significantly influenced how they engage with the world around them, transforming their interactions, learning methods, and overall experiences in manners that were previously uncharted. The internet's pervasive presence has ushered in an era of unparalleled connectivity and information accessibility, fundamentally shaping the way Bhutanese youth navigate and perceive the world. This revelation underscores the imperative to understand and address the unique challenges and opportunities that arise from this digital immersion, ensuring that the benefits of such connectivity are maximized while safeguarding the well-being of Bhutan's young generation.

A significant majority of students and children in Bhutan have ready access to smartphones, with these devices playing a central role in their daily lives. Furthermore, many parents utilize smartphones as a means to engage and entertain their children. Particularly noteworthy is the pivotal role that digital education has assumed, especially during and post-COVID-19 pandemic, further underscoring the growing significance of smartphones and technology in shaping the learning landscape.

A student from the FDG shared, "We usually get our first phones when we're around 13 to 18 years old, and we start using them from around class 7."

Among children and young people, the most popular device for accessing the Internet is the mobile phone. This represents a notable shift over the past decade. In Europe and North America, the first generation of Internet users logged on via desktop computers, but in Bhutan, a significant proportion of young people and students access the Internet primarily through smartphones. Children and young people prefer using mobile phones because they can carry them around everywhere; they do not have to share them with other household members; they can fulfil several functions at the same time, such as texting, talking, clicking and sharing pictures, and surfing; and it is always on.

Children and young people spend on average about two hours a day online during the week and roughly double that each day of the weekend. Some feel permanently connected. But many others still do not have access to the Internet at home – or have only restricted access. However, statistics vary widely and there is a spectrum of views as to how much time children are spending online. Some recent research from the DQ Institute suggests that in Australia children and young people could be spending as much as 38 hours a week online 16. Similarly, in Bhutan, nearly two-thirds (66.3%) of children spend one to three hours per day surfing the Internet. 17 The students from the FGD participants of Bhutan have mentioned that they spend more time, especially on social media. During weekends they spend around 5 to 6 hours on the phone and internet.

In line with the findings from Global Kids Online (GKO) that similar overall numbers of girls and boys have access to the Internet, this trend holds true for Bhutan, where there exists an equitable distribution of Internet access and usage between boys and girls.

¹⁴ ITU (2022), Measuring digital development: Fact and Figures. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

¹⁵ OECD, "New Technologies and 21st Century Children: Recent Trends and Outcomes", Education Working. Paper No. 179.

¹⁶ DQ Institute (2020), Child Safety Index, Https://www.dqinstitute.org/child-online-safety-index/.

¹⁷ MOIC (2021), National ICT Household Survey, Nationwide ICT Household Survey Report.

A world of fun

Children and young people often go online for a variety of positive and enjoyable reasons. Across the 11 countries surveyed, the most popular activity – for both girls and boys – is watching video clips. More than three-quarters of Internet-using children and young people say they watch videos online at least weekly, either alone or with family members. In Bhutan, 79.9% of children with internet access prefer to download and play online games, with this preference being consistent among both urban (80.5%) and rural (79.4%) children. Additionally, about 73.4% of children enjoy streaming and downloading movies, videos, or music from the internet¹⁸.

A significant trend from the Bhutanese students observed among the female participants of FGD is their strong inclination towards watching video content, particularly Korean dramas. One of the female students from FGD shared, "I've really been influenced by K-pop idols and their cuisines. It's made me more introverted, and I've been having a hard time interacting with my friends at school."

On the other hand, a majority of male participants exhibit a keen interest in playing online games, with popular titles like Mobile Legends (ML) and PUBG being particularly favoured. One of the male students from the FGD stated, "I play online games to earn a 999 data package." Interestingly, when it comes to social media usage, there is an equitable level of interest demonstrated by both girls and boys.

Adults worry about children and young people's excessive screen time or believe that they are just wasting time on online entertainment. According to Global Kids Online, these mainstream entertainment activities may provide useful entry-level opportunities for children and young people, which could help them develop the interest and skills to progress further towards more educational, informative and social online experiences.

Making new connections

The Internet, with its instant messaging tools and social networks, has become a crucial meeting point where children and young people can exercise their right to freedom of expression by connecting with their friends and family and with other children and young people who share their interests. Bhutanese students highlight that exposure to social media offers them easier access to information, facilitates communication, allows self-expression, and provides entertainment and motivation. Notably, platforms like TikTok have enabled individuals to achieve fame, earn income, and maintain a sense of pride, showcasing the multifaceted benefits of social media for Bhutan's youth. Online platforms provide avenues for children and young people to connect with others who share their interests and passions.

Online social interactions also increase with age due to various reasons. For instance, some social media websites have a minimum age limit for children and young people, who typically gain more freedom with age. Furthermore, the use of social media is widespread among Bhutanese students, with eight out of ten being knowledgeable about using platforms such as Facebook, Instagram, Snapchat, LINE, and WeChat to share ideas, engage in discussions, and collaborate with peers. However, when it comes to establishing a secure computing environment, including tasks like removing computer viruses and installing security programs or anti-virus software, slightly less than half (46%) of the students possess this capability.

¹⁸ MOIC (2021), National ICT Household Survey, Nationwide ICT Household Survey Report.

With greater access to the Internet, children and young people can widen their horizons, gather information and extend their relationships. With more social interactions, whether online or in-person, they build their experience and skills. GKO research shows that children and young people who socialize more actively on the Internet are better at managing their online privacy, which helps to keep them safe. However, it is crucial to balance online connections with responsible usage. Parents and educators play a vital role in guiding children and young people to make informed decisions while navigating the digital world. By setting guidelines, encouraging critical thinking, and promoting respectful online behavior, adults can help ensure that these connections remain positive and beneficial.

The joy of creation

Some of the online content that children and young people find and value has been produced by other children and young people. Typically, in the 11 countries surveyed by Global Kids Online, 10 to 20 percent of children and young people create and upload their video or music each week, or write a blog, or story, or create web pages every week.

One of the female students from the FGD mentioned, "I take photos and record videos, then share them online as a story."

Many young people and students in Bhutan have shown a keen interest in showcasing their skills and talents by uploading videos online, and some have even seized opportunities through social media platforms. TikTok has emerged as one of the most popular sites for entertainment and video sharing, while YouTube also plays a vital role in providing a platform for young individuals to share their talents and creativity. At least half (52%) of them also engage in posting news and information concerning social issues on online platforms¹⁹.

AN APPETITE FOR INFORMATION

Like adults, children and young people are taking advantage of the Internet to enjoy their right to information. Between one-fifth and two-fifths of children and young people can be considered 'information-seekers', in that they carry out multiple forms of information searches online each week – to learn something new, to find out about work or study opportunities, to look for news, to source health information or to find events in their neighbourhood.

Many children and young people of all ages use the Internet for homework, or even to catch up after missing classes. One of the male students shared, "I utilize the internet to browse for information and gather ideas."

With the digitalization of the education system in Bhutan, many students now use chat sites to discuss and exchange notes with their friends and teachers. The creation of class group chats for disseminating information has proven to be beneficial for both students and educators. More than half of the students (58%) utilize the Internet to address school-related problems. Similarly, 56% use the Internet to solve problems in their town/community²⁰.

Some children and young people are more likely to use the Internet than others to search for information. Data show that the children and young people who use the Internet for a wide range of information-seeking activities tend to be older with the capacity to engage in a broader range of online activities generally and have parents with a supportive and enabling attitude towards their Internet use. This

¹⁹ MoE (2020), Digital Kids Asia Pacific, The Country Report Bhutan.

²⁰ MoE (2020), Digital Kids Asia Pacific, The Country Report Bhutan.

suggests that as children and young people grow older with the right kind of parental support, they tend to gain more online experience and utilise the Internet to their benefit.

With so much information available online, children and young people must have the necessary skills to find the right content and check the truth of what they discover.

There are few differences between girls and boys in this regard, with children and young people getting more expert at finding what they need online by their teenage years. Children and young people who watch more video clips online seem to have better information-seeking skills, perhaps because they learn how to find what they need by searching for online content more frequently.

The quality and quantity of information that children and young people gather online will depend on their interests and motivation. But what they find will also be affected by the extent of the information available, which will be higher for the most widely spoken languages.

It is one thing to be adept at searching for information on the Internet and another to be able to check whether the information found online is true.

When compared with the proportion of children and young people who reported having strong information-seeking skills, there were only a few children and young people who said they were good at critically evaluating the information they found.

One of the male students recounted, "One time, we had an issue where fake news was going around on the Facebook confession page, suggesting that a teacher was having an affair with a student. In the end, it turned out that the child had fabricated the whole thing; there was no truth to it. We ended up having to stay in school for three days while they conducted meetings to identify who had spread the false information. We were completely unaware of the actual situation at the time."

Overall, children and young people do not yet seem to be taking full advantage of the opportunities for searching and checking information online. To do so, younger children especially will need more support, either from their parents, schools or digital providers, to encourage and help them to advance their rights in the digital world.

Becoming active citizens

Beyond seeking information and creating content, children and young people can also engage in civic or political activity via the Internet. According to the Convention on the Rights of the Child, a child has civic rights, including the right to be heard, to express themselves and to meet others. However, it is clear from Global Kids Online research that relatively few children and young people are taking advantage of civic engagement opportunities online.

Young people are most likely to engage politically online. Bhutanese students and young people stay well-informed about politics and current events in the country through social media channels. Some of them take the initiative to create dedicated pages on their social media accounts to disseminate information, while others share updates on their personal accounts and stories. The younger generation today is significantly more knowledgeable about both national and international politics compared to previous generations, thanks to their access to information and engagement through social media platforms.

Running risks and suffering harm

Children and young people are exposed to new risks when online, which could lead them to harm. They may come across information on how to self-harm or commit suicide. They can also be confronted with hate speech or material of a violent or sexual nature. The survey conducted by Global Kids Online across countries suggested that the children and young people who engage in a wider range of online activities had experienced more online risks, perhaps as a consequence of their heightened exposure or their more confident exploration of the Internet. It is important to remember that risk does not always lead to harm. Children and young people exposed to online risks may not suffer harm if they have the knowledge and resilience to cope with the experience. Therefore, it is important to identify who among them is most vulnerable to online harms and what it takes for risks to be translated into harms to effectively protect children and young people online without unduly limiting their opportunities.

Overall, about 20 per cent of children and young people surveyed by Global Kids Online said that they had seen, in the past year, websites or online discussions about people physically harming or hurting themselves, while about 15 per cent of children and young people had seen content related to suicide. It also showed that children and young people had been exposed to hate speech.

Bhutanese students and young people are exposed to a wide range of negative aspects of the internet, including pornography, online fights, online abuse, and cyberbullying. Many of them have witnessed numerous cases of online abuse occurring within their communities and beyond. This exposure highlights the importance of educating and raising awareness among young people about online safety, responsible internet usage, and the potential risks associated with the digital world. It also underscores the need for measures to protect and support them in navigating the online landscape safely.

One of the male students shared, "There are a lot of negative comments made about people online, and girls, in particular, face online bullying from strangers."

Between one-quarter and one-third of children and young people surveyed on the issue had been confronted with violent content online or sexual content in any form of media. Sometimes children and young people came across content of a sexual nature by accident; on other occasions, friends had recommended sexual content, or they had been sent it by others, including strangers. Some children and young people had asked for sexual images from others.

In several countries, many children and young people have experienced a variety of online risks, but far fewer report feeling harmed as a result. The findings vary by country, and young people are somewhat more likely to experience harm than younger children, probably because they spend more time online and tend to be involved in a wider range of online activities.

One of the girls shared her experience, saying, "Once, when I was trying to access a particular website, a pop-up link appeared, and when I clicked on it, it redirected me to a pornographic website."

Children and young people can be treated in hurtful ways both online and offline. On online platforms, damage can be caused either by hurtful or nasty messages by being excluded from group activities or by being threatened. These experiences are often termed as 'cyberbullying'. But children and young people can be similarly hurt in their day-to-day interactions offline. Roughly equal proportions of children and young people bullied by others experience this in person and online.

A male student shared, "The victims of online abuse are often closely observed by their friends and the community, and their academic performance tends to deteriorate as they experience heightened stress."

A girl shared, "I know a victim of online abuse, and they are extremely stressed and depressed, with their self-esteem at an all-time low."

How do children and young people respond to hurtful experiences online? Initially, they turn to their friends or siblings. Then they may tell their parents. Very few children and young people in the countries surveyed will seek support from their teachers. Although young people encounter more risks than younger children, they do not suffer from correspondingly greater harm – suggesting that with experience comes resilience.

A girl mentioned, "I once received inappropriate messages from a boy with malicious intentions. I reported the incident to the teacher, and he was subsequently punished and advised not to repeat such behavior."

It is worth noting that children and young people do not always recognize 'online' and 'offline' as distinct spaces. For children and young people, online experiences – whether good or bad

- are intertwined with the other aspects of their lives.

Privacy is a priority

Privacy is the right of a child, according to the Convention on the Rights of the Child. It is important for attaining autonomy and self-determination and is interlinked with a child's right to information, freedom of expression and participation. Children and young people can protect themselves from exploitation by defending their privacy. They need to carefully manage their digital identities and protect their personal data as much as possible.

Many children and young people report strong privacy skills in managing their interpersonal relationships online – for example, they are aware of the information they should and should not share online or they know how to change their social media privacy settings or remove people from their contact lists. This suggests that early efforts to promote Internet safety among children and young people have been fairly successful. Many children and young people have developed strategies to protect themselves online and are aware that they need to consider certain risks when using the Internet.

Approximately 90% of the Bhutanese students claim to have an understanding of what information is suitable for sharing on the Internet and what should be kept private. About 75% of students are capable of adjusting their privacy settings to safeguard themselves from unwanted online interactions. A majority (81%) of students change their account passwords when they discover that their personal information has been misused, compromised, or accessed without authorization. Conversely, only seven percent indicate a willingness to report such incidents to the Child Helpline. When confronted with online bullying from peers or others, the most commonly employed actions by students include blocking and reporting the individuals involved (60%) and removing the contacts (53%)²¹.

A student mentioned, "I adjust my privacy settings and restrict my Facebook profile to only be visible to friends in order to avoid becoming a target of online abuse and cyberbullying."

²¹ MOE, (2020), Digital Kids Asia Pacific, The Country report Bhutan.

More problematically, children and young people online may expose their private information, photographs and communications to potential abuse and inappropriate and unwanted contact. Children and young people may also make contact with people online whom they subsequently meet in person, though this is still relatively rare. Less than one-quarter of children and young people across all countries have met someone face to face whom they had first got to know online.

Perhaps surprisingly, children and young people mostly enjoy these face-to-face meetings and report feeling happy afterwards – suggesting that they are benefiting from growing their circle of friends in this way. On the other hand, even in the small number of cases where children and young people report being upset by these encounters, there is a cause for concern.

Parents sharing content about their children and young people need to consider how this can affect the child. There are concerns that 'sharenting' (parents sharing information and photos of their children online) can violate a child's privacy, lead to bullying, cause embarrassment, or have negative consequences later in life²². Parents of children with disabilities may share such information in search of support or advice, placing children with disabilities at higher risk for adverse outcomes.

Home is where the Wi-Fi is

One way to ensure that online risks do not result in harm to children and young people is to improve guidance on children and young people's Internet use for parents and others.

One of the students expressed, "Parents are often preoccupied with their phones and don't even take the time to listen to what their child has to say. This also applies to my own parents; they don't seem interested in responding."

In principle, parents are in a strong position to support children and young people's Internet use since children and young people primarily access the Internet at home.

But faced with complex and fast-evolving technologies, many parents do not feel sufficiently confident or competent enough to supervise their seemingly tech-savvy children and young people. Parents are also influenced by popular worries about 'screen time', 'Internet addiction' and 'stranger danger'. The temptation is therefore for parents to focus more on restricting their children and young people's Internet use – for instance, by limiting their time online or by forbidding the use of digital devices in bedrooms, during mealtimes or after bedtime – than on enabling or guiding them to participate more productively online.

In most countries, parents are most involved in younger children's Internet use, helping them to navigate the digital space while at the same time imposing more restrictions on them than on young people. They tend to intervene less as their children grow older, although teenagers would surely still benefit from constructive parental guidance on online opportunities as well as risks. In Bhutan, 89.7% of households across the country use a 4G mobile network to access the Internet. Out of the households that provide Internet access to their children, around 55% actively supervise and monitor their children's online activities, while 46% have established house rules governing Internet usage²³.

One reason why a parent hesitates to get involved in their children and young people's Internet use is that they themselves lack expertise.

²² UNICEF and the Office of Research-Innocenti (2017), Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy, https://www.unicef-irc.org/publication/pdf/child_privacy_chanlleges_opportunities.pdf.

²³ MOIC, (2021), National ICT Household Survey, Nationwide ICT Household Survey Report.

One of the parents expressed, "I was unaware of the dangers our children encounter online. It's alarming to learn about issues like addiction, exposure to inappropriate content, and the impact on their emotional well-being. We require better education on this topic."

In consideration of the above statement, it becomes apparent in the FGDs with parents that a number of Bhutanese parents possess limited or minimal knowledge about the online risks their children encounter. This underscores the pressing need for heightened awareness and education concerning these risks. Online violence can yield substantial consequences, including addiction, financial implications, exposure to inappropriate content, and adverse effects on emotional well-being.

CHILDREN WITH VULNERABILITIES

Children and young people can be vulnerable for a variety of different reasons. Research carried out in 2019²⁴ stated "that vulnerable children's digital lives seldom receive the same nuanced and sensitive attention that "real life" adversity tends to attract. Furthermore, the report goes on to say that at best they [children and young people] receive the same generic online safety advice as all other children and young people, while specialist intervention is required".

Although the three examples of specific vulnerabilities are highlighted here, (migrant children, children with autism spectrum disorder and children with disabilities), there are many others.

Migrant children

Children and young people from migrant backgrounds often come to one country (or already live there) with a particular set of socio-cultural experiences and expectations. While technology is usually thought to be a facilitator to connect and participate, online risks and opportunities can differ greatly across contexts. Furthermore, empirical findings and research²⁵ show a vital function of digital media in general:

- It is important for orientation (when travelling to a new country).
- It is a central function for appropriation and being acquainted with the society/culture of the receiving country.
- Social media can play a key role in maintaining contact with family and peers, and for accessing general information.

Alongside the many positive aspects, digital media can also bring challenges for migrants including:

- Infrastructure it is important to think about safe spaces online so that migrant children and young people can benefit from privacy and safety.
- Resources migrants spend most of their money on prepaid phone cards.
- Integration alongside having access to technology, migrant children and young people also need to receive a good digital education.

²⁴ Adrienne Katz (2018), Vulnerable Children in a Digital World, https://pwxp5srs168nsac2n3fnjyaa-wpengine.netdna-ssl.com/wp-content/uploads/2019/02/Vulnerable-Children-in-a-Digital-World-FINAL.pdf.

²⁵ Better Internet for Kids (2017), Report on the proceedings of the Safer Internet Forum 2017, https://www.betterinternetforkids.eu/documents/167024/1738388/Report+on+the+proceedings+of+the+Safer+Internet+Forum+2017/fa4db409-4fae-45b1-96ec-35943b7d975d

Children with Autism Spectrum Disorder (ASD)

The autism spectrum summarises two core domains in the DSM-5²⁶ behaviour diagnostic process.

- Restricted and repetitive behaviour (the need for sameness).
- Difficulty with social and communicative behaviours.
- Frequent co-occurrence with intellectual disability, language issues and similar.

Technology and the Internet offer endless opportunities for children and young people when learning, communicating and playing. However, alongside these benefits, there are many risks that children and young people with ASD may be more vulnerable to, such as:

- The Internet can give children and young people with autism opportunities for socialising and special interests that they may not have offline.
- Social challenges, such as difficulty with understanding others' intentions, can leave this group vulnerable to 'friends' with bad intentions.
- Online challenges are often connected to core characteristics of autism: concrete, specific guidance could improve individuals' online experiences, but the underlying challenges remain.

Children with disabilities

According to some of the first consultative research on children with disabilities' experiences in the digital environment, these children felt that, in many ways, their digital and online lives were very similar to those of children without disabilities. Nevertheless, there were a number of distinct and important differences²⁷. While considering these, it is important to bear in mind that the challenges and barriers faced by children with disabilities vary significantly, according to the type and nature of impairment. Their particular needs should be considered on an individual basis.

Children and young people with disabilities face risks online in similar ways to children and young people without disabilities, but they may also face specific risks related to their disabilities. They are 12 per cent more likely to have experienced cyberbullying than children and young people without disabilities. Some children and young people with disabilities may be less skilled in managing their interpersonal relationships online or distinguishing between true and false information. Some could also be easily manipulated into spending money, sharing inappropriate information, etc. Children and young people with disabilities often face exclusion, stigmatization, and barriers (physical, economic, societal and attitudinal) in participating in their communities. These experiences can have a negative impact on a child with a disability seeking out social interactions and friendships in online spaces, which otherwise could be positive, assist in building self-esteem, and create support networks. However, it can also place them at higher risk for incidents of grooming, online solicitation, and/or sexual harassment. Research shows that children and young people experiencing difficulties offline and those affected by psychosocial difficulties are at heightened risk of such incidents²⁸.

²⁶ Cardwell C. Nuckols (2013), The Diagnostic and Statistical Manual of Mental Disorders, https://dhss.delaware.gov/dsamh/files/si2013_ds-m5foraddictsmhandcriminaljustice.pdf.

²⁷ Lundy et al. (2019), TWO CLICKS FORWARD AND ONE CLICK BACK: Report on children with disabilities in the digital environment, https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

²⁸ Andrew Schrock et al. (2008), Solicitation, Harassment, and Problematic Content, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.

Perpetrators of grooming, online solicitation, and/or sexual harassment towards children and young people with disabilities can include not only preferential offenders who target children and young people but also those who target children and young people with disabilities. Such offenders may include 'devotees' – nondisabled persons sexually attracted to persons with disabilities (most commonly amputees and persons using mobility aids), some of whom even pretend to be disabled themselves²⁹. Actions by such people may include downloading photos and videos of children and young people with disabilities (that are innocuous in nature), and/or sharing them through dedicated forums or social media accounts. Reporting tools on forums and social media often do not have an appropriate pathway to deal with such actions.

Some children and young people with disabilities may face difficulties in using, or even exclusion from online environments due to inaccessible design (e.g. apps that do not allow text size to be increased), denial of requested accommodations (e.g. screen reader software or adaptive computer controls), or the need for appropriate support (e.g. coaching in how to use equipment, one on one support to navigating social interactions)³⁰.

Some parents of children and young people with disabilities may be overprotective because of their lack of knowledge on how to best guide their child's use of the Internet or protect them from bullying or harassment³¹. Some parents of children and young people with disabilities may share information or media (photos, videos) of their child in pursuit of support or advice, placing their child at risk for privacy violations both now and in the future. This also carries the risk of such parents being targeted by uninformed or unscrupulous people offering treatments, therapies, or 'cures' for their child's disability³².

NEW AND EMERGING RISKS AND CHALLENGES

Internet of Things

The Internet has changed the way people live. It provides access to the entire sum of human knowledge, anytime, anywhere. For some, life is much easier and much more 'comfortable' than it has ever been. But this shift has also destroyed some of the traditional lifestyles whether in business or personal lives. For instance, some former business models have been completely changed or negated and, on a personal level, face-to-face interactions seem to have been diminished by the rise of the Internet.

It is important to consider the open Internet and the Internet of Things: the open Internet is merely virtual; it doesn't exist in everyday reality and it is a choice to interact with it. This is not true with the Internet of Things where physical objects are imbued with the life of connectivity, intended to improve our lives – a tweeting toaster is just one such example!

The possibilities of the Internet of Things (IoT) are innumerable. Already IoT is available in wearables, lights in the house, cameras, cars, toilets, packaging, energy meters, medical sensors... the list is endless. The IoT has the potential to change everything for the better. Indeed, some regard it as embedded in the 'fourth industrial revolution'.

²⁹ Richard L Bruno (1997), Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder, Sexual and Disability, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.

³⁰ UNO (2008), Convention on the Rights of Persons with Disabilities and Optional Protocol, https://www.un.org/disabilities/documents/convention/convoptprot-e.pdf. For guidelines on these rights, see Article 9 on Accessibility and Article 21 on Freedom of expression and opinion, and access to information.

³¹ Lundy et al. (2019), TWO CLICKS FORWARD AND ONE CLICK BACK: Report on children with disabilities in the digital environment, https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with.

³² Sonia Livingstone et al. (2019), UNICEF Innocenti Research Brief: Is There a Ladder of Children's Online Participation?, https://unicef-irc.org/publications/pdf/IRB_2019-02%2013-2-19.pdf.

When these items are used in the vicinity of children (i.e. in their homes) they could be exposed to risks such as those associated with using smart wearables or clothing, which could potentially share their location

There are massive market opportunities. However, there are also some potential problems:

Technical/Privacy problems

- Device security proper security can be relatively expensive; and susceptible to viruses/ malware.
- Communications security encryption is weaker as energy is the limiting factor. Susceptible to manipulation by third parties/identity theft etc.
- Always-on communications there is an increasing reliance on devices that rely on always-on communications.
- Data safety in the cloud realistically you have no idea who is using your data.

Social problems

- Exclusion of people.
- Potential for abuse of data.
- Potential for technology to facilitate domestic abuse situations³³.

Economic problems

Job loss.

Environmental problems

• Pollution at every stage (50 billion devices within five years from now).

CONNECTED TOYS AND ROBOTICS

With the growth in technological advancement, there have been fundamental changes in human life that tend to not only apply to adults but, thanks to the emergence of the "Internet of toys", to children and young people, too. As more and more aspects of our lives are transformed into computerised data, consideration needs to be given to how to protect children and young people and provide them with opportunities to grow up in a safe and secure digital world.

Opinions on robotics have changed and there has been much debate around the 'robotification' of childhood³⁴. Once seen as dull, dirty, dangerous, industrial and a threat to labour in factory environments, robots have evolved into a tool that is considered to be sophisticated, supportive and social and something that can be interacted with in homes and in leisure time. While toys have long been fashioned as robots, there have been tremendous changes making the robots more sophisticated. They are no longer just taking the shape and form of the classic science fiction robot, but now coming to life as walking, talking and thinking toys.

³³ Julie Inman Grant, 2019, When "smart" is not necessarily safe: the rise of connected devices extending domestic violence, https://www.esafety.gov.au/about-us/blog/when-smart-not-necessarily-safe-rise-connected-devices-extending-domestic-violence.
³⁴ Jochen Peter at the Safer Internet Forum 2017: Better Internet for Kids (2017), Report on the proceedings of the Safer Internet Forum 2017, https://www.betterinternetforkids.eu/documents/167024/1738388/%20Report+on+the+proceedings+of+the+Safer+Internet+Forum+2017/fa4db409-4fae-45b1-96ec%20-35943b7d975d

There have been some significant technological changes behind robotification, which can be summarised as follows:

- Exponential increases in computing power.
- Mobile connectivity.
- Datafication and networked information.
- Miniaturisation of sensors, microphones, and cameras.
- Robotic cloud computing.
- Progress in artificial intelligence and machine learning.

Perhaps one of the most common robots that children and young people interact with today is Siri; amusing as a conversation with a digital assistant might be, it shows the depth of maturity behind the artificial intelligence (AI) and algorithms that drive it. A social robot can be defined as "An artificial, embodied device that can sense its (social) environment and purposefully and autonomously interact with (agents in) that environment following social rules attached to its role." Social robots may be especially appealing to children and young people as they are early adopters of new technologies and are often targeted as users of new technologies. In addition, children and young people typically have an emerging but scattered field of diverging interests. As a result, however, children and young people are probably more susceptible to the effects of interacting with robots.

Typical features of child-robot interaction include:

- Mobility.
- Interactivity/Reciprocity.
- "Naturalisation" (speech, gestures, and vision rather than text).
- Adjustability of interaction.
- Personalisation.
- (Dis-)Embodiment.

While processes reflect:

- Anthropomorphism (displaying human characteristics or behaviour).
- Social presence.
- Involvement.
- Perceived similarity.

There are a range of potential consequences for the cognitive development of children and young people, which stem from their interaction with robots, both positive and negative. Positive outcomes include improved learning, which is personalised to the child, continuously updated and facilitates self-learning. Less positive outcomes stem from "educational bubbles" which are similar to the "filter bubbles" on the Internet where content is restricted. In such instances, there is a risk of fragmentation in the child's knowledge and delivery of an abundance of facts, while the teaching style is based purely on algorithmic learning. For example, when a child asks Alexa a question (much as they might ask Google or Bing a question), they only receive one answer, making it difficult for them to be able to critically assess the content that they are presented with.

Similar concerns also apply to the ³⁵identity development of the child. Research-based studies have shown that robots can play an important role in the lives of children and young people by helping them to expand and improve their identity search throughout their adolescence. However, robots raise privacy issues, and there is a risk that they may be used as surveillance machines for instance, using them to record anyone within its proximity and hence raising significant safety concerns for both parents and children and young people.

When it comes to relational aspects, relationships with robots might not always reflect real relationships in real life. On the one hand, this might lead to children and young people getting isolated from society, finding comfort in an algorithm that soothes and comforts him or her. However, it could also mean that robots can provide a retreat to "discuss" things that are difficult to bring up in a conversation with parents and peers. Our relationship with robots will always be a servant/master relationship, but robots can increasingly "pretend to feel" and therefore, children and young people might fall into the trap of considering this relationship authentic and mutual. As Jochen Peter stated, "Robots have more to offer than traditional toys but they also present massive risks for the youngest users"³⁶.

ONLINE GAMING

The gaming industry has surpassed both movies and music in terms of customers and revenue. Moreover, with the advent of mobile gaming which can be accessed on a small mobile device, more people are playing games than ever before. The State of Online Gaming 2019 research highlights that 51.8 percent are male gamers and 48.2 percent are female gamers, based on responses from 4 500 consumers in France, Germany, India, Italy, Japan, Singapore, the Republic of Korea, the United Kingdom, and the United States of America, age 18 and older who play video games at least once a week³⁷. And 21 percent of video game players are under 18 years of age in the United States of America since 2010³⁸. Similarly, in Bhutan, nearly eight out of ten (79.9%) children opt for downloading and playing games online. This preference for downloading and playing games is consistent among both rural and urban children, and there is an equal ratio of online gamers among both males and females³⁹.

Recent research in France, Germany, Spain, and the United Kingdom found that 54 per cent of all those aged between 6 and 64 play video games with 77 percent of them playing for at least an hour a week. Moreover, three-quarters of 6 to 15-year-olds in Germany, Spain, Italy, the United Kingdom, and France are video game players; these account for over 24 million across five GameTrack European markets. They play a variety of devices but around 7 in 10 gamers play on either consoles or smart devices⁴⁰.

Across the world, there are more than 2.5 billion video gamers. The game PUBG had the highest peak number of players with 3 million players in 1 hour⁴¹.

³⁵ Van Straten, C. L., Peter, J., & Kühne, R. (2019). Child-robot relationship formation: A narrative review of empirical research. International Journal of Social

³⁶ Van Straten, C. L., Peter, J., & Kühne, R. (2019). Child-robot relationship formation: A narrative review of empirical research. International

³⁷ Limelight Networks (2019), Market Research: The State of Online Gaming, http://img03.en25.com/error.aspx?aspxerrorpath=/Web/%20 LLNW/{02ca9602-173c-43a4-9ee1-b8980c1ea459}_SOOG2019_MR_8.5x11.pdf.

³⁸ Statista.com (2019), U.S. Average Age of Video Gamers in 2019 | Statista, https://www.statista.com/statistics/%20189582/age-of-us-video-game-players-since-2010/

³⁹ MOIC, (2021), National ICT Household Survey, Nationwide ICT Household Survey Report.

⁴⁰ Isfe.eu (2019), GameTrack In-Game Spending in 2019, https://www.isfe.eu/wp-content/uploads/2019/12/%20GameTrack-In-Game-Spending-2019.pdf.

⁴¹ WEPC (2018), 2018 Video Game Industry Statistics, Trends & Data - The Ultimate List, https://www.wepc.com/news/video-game-statis-tics/

One of the leading platforms for viewing gaming video content worldwide is Twitch which accounted for 54 per cent of the gaming video content platform revenue in 2017.

In-game purchases are an increasingly important part of online gaming. With improved Internet connectivity and speed, more players are downloading their games rather than buying a physical copy. In South Africa, online transactions have increased by 13 per cent for gamers from 2018 to 2019⁴².

A boy shared, "I make payments to a third party to acquire in-game items for PUBG."

Alongside the range of mobile gaming, there has also been a huge growth in online gaming. Not all games can be played online but all gaming consoles are able to go online now. Playing online games also means that users can be playing games alongside others on the Internet. Some games only allow users to play with people with whom they are "friends", but others can group you with other players from across the world – sometimes randomly and sometimes based on skill level or preferences.

There are a number of different types of games available and these are constantly changing. Some of the popular games and genres are listed below:

First-person shooter (FPS) – action games focused on gun or projectile-based combat through a first-person viewpoint e.g. Call of Duty, Overwatch, BioShock, Battlefield

Action – adventure – games in which the player traverses and explores environments often involving combat and puzzle-solving e.g. Grand Theft Auto (GTA), Super Mario, Uncharted, The Legend of Zelda, God of War

Sports – Games that stimulate the strategy and physics of real-world professional sports e.g. FIFA, Madden NFL, NBA

Sandbox/Open World – Games involving minimal or no storytelling or limitations, letting the player freely roam and change the virtual world at will e.g. Minecraft, Terraria, Skyrim, Fallout

Multiplayer Online Battle Arena (MOBA) – online games played as two competing teams attempting to capture or destroy each other's base e.g. Dota 2, League of Legends, Heroes of the Storm, Paragon

There are concerns about online gaming addiction which was defined as gaming disorder by the World Health Organisation in 2018⁴³. This has been defined in the 11th revision of the International Classification of Diseases as a pattern of gaming behaviour ("digital-gaming" or "video-gaming") characterized by impaired control over gaming, increasing priority given to gaming over other activities to the extent that gaming takes precedence over other interests and daily activities, and continuation or escalation of gaming despite the occurrence of negative consequences. It is important to note that in order for gaming disorder to be diagnosed, the behaviour patterns associated with it would need to be seen for at least 12 months.

Another key concern with gaming is the link to online gambling. Some games encourage users to take a chance on loot boxes for example, where a player buys a box using in-game currency (in-game currency is purchased using real money) in order to receive a randomised reward⁴⁴.

Recent research has found that the global loot box market is estimated to be worth £20 billion⁴⁵.

⁴² Chris Cleverly (2019), Mobile Gaming in Africa, https://medium.com/kamari-coin/mobile-gaming-in-africa-cc8bb6d7c49b.

⁴³ WHO (2018), WHO | Gaming Disorder, https://www.who.int/features/qa/gaming-disorder/en/

⁴⁴ Parentzone.org.uk (date?), What Are Loot Boxes?, https://parentzone.org.uk/article/what-are-loot-boxes.

⁴⁵ RSPH (2019), Skins in the Game A High-Stakes Relationship between Gambling and Young People's Health and Wellbeing?, https://www.rsph.org.uk/uploads/assets/uploaded/a9986026-c6d7-4a76-b300ba35676d88f9.pdf.

Artificial intelligence and machine learning

Artificial intelligence generates a lot of interest from the media. The applications of Al that are being tested are becoming more wide-ranging. Al also triggers concerns and worries about the negative biases that Al can have.

It is important to define AI and machine learning but there is no universal and versatile definition available. It depends on the purpose, the focus and the specific tasks. This variety of definitions also reflects the diverse definitions of "human intelligence". There is also a difference between specific and general tasks: humans are good at general tasks, while for specific tasks, AI is really advanced.

With the advent of AI in Bhutan, the younger generation has become deeply entrenched in the internet and heavily reliant on it. The traditional practice of creating art has been supplanted by AI-generated art, and tasks such as writing have become significantly more streamlined. However, this heavy dependence on technology has started to take its toll on Bhutan's youth. They have become so reliant on it that it is beginning to impede their development, particularly in terms of critical thinking and analytical skills.

Machine learning most often refers to methods where machines can learn based on data. It aims to generalise data to create models. Machine learning represents 80 per cent of the current AI applications.

There are a number of issues to consider when it comes to Al:

- Ill-defined problems problem definition is key to success.
- Data availability very often, the data is wrong, not appropriate, "dirty", or not enough. Data used to train and develop AI and algorithmic services are likely to be gained from adult users. This may mean that algorithmic decision-making systems and pattern recognition that use AI may be very adult-centric and therefore result in services that misunderstand/ wrongly categorise risks/ behaviour by children. In a similar way, the data sets and models used to shape and inform AI decision-making processes may not accurately represent or consider the needs of some people due to their ethnicity, gender, disability etc. Therefore, children in these underrepresented groups may experience additional, intersectional disadvantage that is further compounded or exploited by AI.
- Neglecting comprehension sometimes, things work by chance or a model is good, but for something other than the initial problem – for example, there have been stories in the media reporting when AI has misidentified images in searches⁴⁶.
- The cost of mistakes.

Artificial intelligence is an amazing development, but the conundrum it generates is similar to that of a self-driving car⁴⁷.

⁴⁶ James Vincent (2019), If You Can Identify What's in These Images, You're Smarter than AI, https://www.theverge.com/2019/7/19/20700481/ai-machine-learning-vision-system-naturally-occuring-adversarial-examples

⁴⁷ Amy Maxmen (2018), Self-Driving Car Dilemmas Reveal That Moral Choices Are Not Universal, https://www.nature.com/articles/d41586-018-07135-0.

UNDERSTANDING RISKS AND HARMS

Table 1 shows a classification of online risks to children. It is acknowledged that there are also health and well-being-related risks (excessive use, sleep deprivation etc.).

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)

Content

- Exposure to illegal and/or potentially harmful content, such as pornography, gambling, self-harm
 websites and other content inappropriate for children and young people. In most cases, operators
 of these websites do not take effective measures to restrict access to children and young people.
- Exposure to contact with other users.
- Self-harm, destructive and violent behaviours.
- Exposure to radicalisation, racism and other discriminatory speech and images.
- Relying upon or using inaccurate or incomplete information found online, or information from an unknown or unreliable source.
- Creation, reception and dissemination of illegal and harmful content.

Online manipulation

Children and young people are ever more present in the online environment such as social networks where they are exposed to a variety of content, algorithmically filtered, with an intention to manipulate them in one way or another. Examples include political manipulation (promoting certain political points of view), fake news (spreading false information with political, commercial or other intentions), and advertising (creating early attachment of children and young people towards specific brands or products).

COP is a top priority for telecommunications companies, including Bhutan Telecom and TashiCell. They both recognize the importance of safeguarding children when providing internet access, social media platforms, gaming, messaging, and other services. Age verification processes and content filtering systems are in place to ensure age-appropriate access and block harmful content. They also collaborate with educational institutions and organizations to promote digital literacy and online safety programs for children.

Although the security providers have implemented some of the basic filter systems, there are more safety systems required. Implementing more filters and safety features in the service provider industry poses several challenges. These include the need for technological expertise, resource allocation, maintaining a positive user experience, navigating regulatory compliance, aligning with business strategy, addressing false positives and negatives, staying adaptable in a changing digital landscape, respecting user privacy, and establishing effective feedback mechanisms. Striking the right balance between filtering and usability while considering these factors is essential for service providers seeking to enhance their operations without hampering their business strategy.

These algorithmically customized environments can greatly influence children and young people's healthy development, opinions, preferences, values and habits by isolating them in "filter bubbles" and preventing them from freely exploring and accessing a wide variety of opinions and content.

Contact

Pretending to be someone else, often another child, as part of a deliberate attempt to harm, harass or bully someone else.

Online solicitation or grooming

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) provides that grooming (solicitation of children for sexual parties) is the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the legal age for sexual activity, for the purpose of committing acts of sexual abuse or producing child sexual abuse material⁴⁸. The solicitation does not necessarily result in a meeting in person. It may remain online and nonetheless cause serious harm to the child, for example through the production, possession and transmission of child sexual abuse material⁴⁹.

In the context of sexual solicitation, or grooming, there is more focus on the process of victimization because the research has largely involved children and young people themselves.

The limited awareness of online child grooming risks among Bhutanese households, with only 12.3% being informed, highlights a concerning issue⁵⁰. Many households lack the necessary skills to guide and protect their children from online dangers, including harmful content. To address this issue, various stakeholders, including the government, NGOs, and other sectors, are actively working to educate and inform the population about the risks associated with online grooming and other threats.

Bullying and harassment.

Bullying is bullying wherever and however, it happens. Online bullying can be particularly upsetting and damaging because it tends to spread more widely, with a greater degree of publicity. Moreover, the content circulated electronically can resurface at any time, which makes it harder for the victim of the bullying to get closure over the incident; it may contain damaging visual images or hurtful words; the content is available 24 hours a day. Bullying by electronic means can happen 24/7, so it can invade the victim's privacy even in otherwise 'safe' places such as at home, personal information

⁴⁸ Council of Europe (1957), Article 23 of the Treaty No. 201: Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, https://www.coe.int/en/web/conventions/full-list.

⁴⁹ Committee of the Parties to the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2015), Opinion on Article 23 of the Lanzarote Convention and its explanatory note, http://rm.coe.int/coermpubliccommonsearchservices/displaydctmcontent?documentid=090000168064de98

⁵⁰ MOIC, (2021), National ICT Household Survey, Nationwide ICT Household Survey Report.

can be manipulated, visual images altered, and forwarded to others. Further, it can be carried out anonymously⁵¹.

Creating fake accounts, and sharing inappropriate content, "I've seen some of my classmates engage in cyberbullying on social media. They spread rumors and say hurtful things to others. It creates a toxic environment, and it's disheartening to witness", shared by a student.

The consultative meeting with stakeholders shed light on the serious issue of cyberbullying affecting children, involving harassment, threats, and humiliation. These acts can have severe consequences, including anxiety, depression, reduced self-esteem, and a reluctance to participate in online activities or attend school.

Children and young people who are victimized offline are likely to be victimized online⁵². According to recent studies, children with disabilities are more likely to experience abuse of any kind⁵³, and specifically are more likely to experience sexual victimization⁵⁴, placing them at a higher risk online. Victimization can include bullying, harassment, exclusion, and discrimination based on a child's actual or perceived disability, or on aspects related to their disability such as the way that they behave or speak, or the equipment or services they use. Some of the risks can involve:

- Defamation and damage to reputation.
- Unauthorised use of credit cards: the credit cards of parents or others which can be used to pay for membership fees, other service fees and merchandise.
- Criminal attempts to impersonate Internet users, primarily for financial gain. In some instances, this might include identity theft, although this is normally associated with attempts to defraud adults.
- Unwanted advertising: some companies spam children through websites to sell products. This
 raises the issue of user consent and how this should be obtained. There is insufficient legislation in
 this area, and it is very difficult to determine when children and young people are able to understand
 data transactions. Indeed, how to apply these rules on the Internet is already a major concern and
 mobile phone access accentuates the problem.
- Undesirable contact, especially with adult impostors posing as children and young people.

Conduct

- Disclosure of personal information leading to the risk of physical harm.
- Physical harm through real-life encounters with online acquaintances, with the possibility of physical and sexual abuse.
- 'Sexting', is the sharing of intimate images that can result in sexual harassment, sextortion, grooming and image-based abuse⁵⁵.

⁵¹ Dr Tanya Byron (2008), The Report of the Byron Review: Safer Children in a Digital World, https://www.education.gov.uk/publications/%20eorderingdownload/dcsf-00334-2008.pdf.

⁵² Schrock et al. (2008), Online Threats to Youth: Solicitation, Harassment, and Problematic Content, http://cyber.harvard.edu/sites/cyber. law.harvard.edu/files/RAB Lit Review 121808 0.pdf.

⁵³ UNICEF (2013), State of the World's Children Report: Children with Disabilities, https://www.unicef.org/%20publications/files/sowc2013_exec_summary_eng_lo_res_24_apr_2013.pdf.

⁵⁴ Mueller-Johnson, Eisner and Obsuth (2014), Sexual Victimization of Youth With a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors, http://journals.sagepub.com/doi/10.1177/%200886260514534529.

⁵⁵ Lanzarote Committee (2019), Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children, https://rm.coe.int/opinion-of-the-lanzarote-committee-on-child-sexually-suggestive-or-exp/168094e72c

Sexting

A common behaviour by teenagers is 'sexting' (sharing of sexualized images or text via mobile phones). These images and text are often shared between partners in a relationship or with potential partners, but sometimes end up being shared with much wider audiences. It is thought unlikely that young teenagers have an adequate understanding of the implications of these behaviours and the potential risks they entail⁵⁶.

A serious concern with sexting is that children and young people may be creating illegal child sexual abuse material, which could lead to serious legal sanctions. Some of the dangers include:

Targeting through spam and advertisements from companies using Internet sites to promote age and/ or interest-targeted products.

Conduct resulting in health risks such as screen time: Compulsive and excessive use of the Internet and/or online gaming, to the detriment of social and/or outdoor activities important for health, confidence building, social development and general well-being.

Infringement of their own rights or the rights of others through plagiarism and uploading content (especially photos) without permission. Taking and uploading inappropriate photos without permission has been demonstrated to be harmful to others.

Infringement of other people's copyright e.g. by downloading music, films or TV programmes that ought to be paid for.

Misrepresentation of a person's age: either a child pretending to be older to gain access to age-inappropriate websites or an older person pretending to be a child.

Use of parent's email account without consent: parental consent is required to activate some online accounts, which can be difficult for parents to delete once activated. Children and young people use this method to circumvent permission.

The EU Kids Online 2020 survey illustrates how children and young people are using new media

– As opposed to how people think they are using it⁵⁷. Other research explores how children think that their rights should be protected in the digital environment⁵⁸ as well as works on the experiences of children with disabilities⁵⁹.

The main objective of an online safety campaign is to change behaviour, including encouraging safer online behaviour by children and young people, encouraging effective online parenting and encouraging others who interact with children and young people to teach them to stay safe online (extended family members, teachers, etc.).

Children and young people's Internet safety should not be seen in isolation but rather as one that has commonalities within a range of initiatives concerning children and young people, their safety and the Internet.

⁵⁶ UNICEF (2011), Child Safety Online: Global Challenges and Strategies, http://www.unicef.it/allegati/child_safety_online_1.pdf.
⁵⁷ Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids

Online 2020: Survey results from 19 countries. EU Kids Online, http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf.

⁵⁸ Council of Europe (2017), It is Our World: Children's Views on How to Protect Their Rights in the Digital World, https://rm.coe.int/it-s-our-world-children-s-views-on-how-to-protect-their-rights-in-the-/1680765dff.

⁵⁹ Lundy et al. (2019), TWO CLICKS FORWARD AND ONE CLICK BACK: Report on children with disabilities in the digital environment, https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

THE ROLE OF PARENTS, CARERS AND GUARDIANS CAN PLAY

Parents need to support their children and young people so that they can benefit from technology safely. They should have a balanced approach and recognise the wide range of benefits that the Internet can provide. Parents may be inclined to focus on the many positive educational/skills benefits that can be gained online but it is important that they also consider and appreciate the social benefits that children may gain - play and exploring personal interest can be key motivators for children to use the Internet. Having an understanding of these may help parents to better engage and support children. In order to ensure that children and young people use Internet sites safely and responsibly, parents, carers, and guardians should be aware of the following:

- 1. Familiarise themselves with the risks and opportunities that their children and young people may encounter online. It's important to be able to recognise the potential threats their children may face, whilst remembering that the risks may not result in harm.
- 2. Stay actively engaged in what their children are doing online, the type of content they are watching, sharing or creating, the services, platforms and games they are using, and the people that they are connecting with. It's always helpful for parents to try out the services their children are using.
- 3. Parents should familiarise themselves with good websites and games for learning and entertainment that they can use with their children. A good website or game will have a dedicated safety page with clear links, reporting mechanisms and guidance for children and young people and their parents/carers.
- 4. Have a regular, honest and open dialogue with children and young people that is age-appropriate and changes over time.
 - a. Make sure children and young people understand the risks they may come across and agree on the actions they will take if they encounter them this could be simply talking to you.
 - b. Encourage children and young people to think about how they can be good digital citizens, thinking about what they share about themselves and others, helping them adopt a positive way of behaving online.
 - c. Encourage critical thinking about what they see online, talk about how not everyone is who they say they are, or what they see may not be true. Talk about self-image manipulation and fake news that seeks to exploit people.
 - d. Talk about peer pressure and the fear of missing out and managing friendships online.
 - e. Talk about the lure of addictive and immersive technology, particularly on free services, where the time they spend online and the data they share is the currency or business model.
- 5. Ensure that the child knows when and where to get help. This could be their parent or carer, a teacher or another trusted adult. Foster an attitude that if they experience anything upsetting online, they should discuss it with a trusted adult.
- 6. Agree on family rules for the use of connected devices, understanding that parents or carers are role models for online behaviour.

- 7. Ensure that the children have a balanced digital diet, such that their time online is time well spent and contains a mix of activities that include learning, creating and connecting in positive ways. Use in-built tools to review usage patterns around how much time is spent on apps and services.
- 8. Make sure you and your children are capable tool users. There are numerous tools that can assist parents with the 'management' of connected technology both in and out of the home.
 - a. Consider all connected devices, not just the obvious smartphones, tablets and PCs. Include game consoles, personal assistants, connected televisions, and any other devices that connect online.
 - b. Use age ratings to help decide what content, games, apps and services children and young people have access to. Be aware that age ratings may differ in app stores and actual platforms themselves. Consider using settings to control what apps and games can be downloaded and used.
 - c. Look to use network filtering, often referred to as parental controls, and safe search engines or controls to filter content that children and young people can access online.
 - d. As a family, understand how and when to report any content that they are unhappy, worried or concerned about or that they feel breaks the terms and conditions. Know how to block unwanted or unsolicited contacts.
 - e. Think very carefully about the use of monitoring apps and technologies that track a child's Internet use. They can have unintended consequences of driving more secretive behaviour online and can also cause harm in domestic and family violence situations. If you do use them, explain to your child what you are monitoring and why.
 - f. Importantly, as children and young people age and mature, reassess the use of controls and restrictions to ensure they are age-appropriate; it is important to foster resilience in your child to be able to thrive online.
- 9. Teach your children not to share their access passwords with friends or siblings. Think about when and where they are sharing personal information, for example, a profile that can be seen globally might want to use a non-personal profile picture and minimise personal information around age, school, and location.
- 10. Don't assume everyone on the Internet is targeting your child. In general, children's websites can be safe and can provide a wonderful, creative social and educational experience for your child, but remember to stay involved and aware.
- 11. Stay calm and don't jump to conclusions if you hear or see anything that concerns you about your child's behaviour or the behaviour of one of their online friends. Avoid threatening to remove or confiscate devices as they can be social lifelines for some young people. If your child fear that you will remove them, they are likely to be increasingly reluctant to share problems or concerns that they may have.
- 12. Recovery and learning from experiences are vital elements of developing digital resilience. If children experience risk or harm online, parents can help their children to find ways to recover so that they are able to safely benefit from the positive aspects when appropriate and avoid exclusion where possible.

Where to go for help?

Many countries have helplines where children and young people can report a problem. These are widely publicised and different countries have different approaches to getting this message out. It is important that children and young people realise that it is never too late to report a problem and that by doing so they may help others. The toll-free number 1098 continues to function as a vital helpline in Bhutan, providing support to children in need. This has streamlined and enhanced the effectiveness of the helpline, ensuring that children can access the necessary support and assistance promptly.

The ICM Act of Bhutan, emphasizes the responsibilities of service providers and users in protecting children from exposure to harmful content and online exploitation. It mandates the establishment of mechanisms for reporting and removing child sexual abuse material and encourages cooperation between stakeholders to address child online protection issues effectively. The act also emphasizes the role of education and awareness programs to empower children, parents, and educators with the knowledge and skills necessary to navigate the online world safely.

While children and young people acknowledge that they sometimes allow themselves to engage in risky behaviour, they do not show a lot of anxiety about the inherent risks of this type of behaviour and show a preference for trying to solve the problems by themselves or within their peer group.

A concerned parent expressed, "Children often find it difficult to confide in adults and tend to keep their problems to themselves, attempting to resolve them on their own. They feel more at ease discussing things with their friends rather than with us."

This suggests that they turn to their parents or other adults only in cases of potentially 'dramatic' problems. This is a problem, particularly with older boys who may be more likely to only use a 'Report Abuse' button⁶⁰ (such as developed by the Virtual Global Task Force) instead of additionally reaching out to parents or other adults. However, this is not the case with all children and young people. We can see that children and young people who are aware of risks, do police their own activities but often do not share a view of the new technologies that implies that adults should be the focal point for judging and monitoring children and young people's behaviour⁶¹. There is a need to be cautious about making simple distinctions between offline and online worlds, as this no longer captures how our everyday lives have become, increasingly associated with online technologies. For many children and young people, this means a careful negotiation between the opportunities that technology offers (such as exploring their identity, establishing close relationships and increased sociability) and risks (regarding privacy, misunderstandings and abusive practices) afforded by Internet-mediated communication⁶².

Participant from the RBP, "There have been no reported cases specifically related to cyberbullying or other related issues at the moment. However, we are increasingly recognizing that the likelihood of such cases occurring in the future is high. With the continued advancement of technology and more individuals, including children, engaging in online activities, the risk of cyberbullying is becoming more prevalent." The RBP representative continued, "One of the reasons there aren't any reports is because people aren't aware that they can report internet harassment and threats to the police. Many individuals, including children, feel ashamed about coming forward and reporting these incidents.

⁶⁰ Europol (2019), 2019 Virtual Global Taskforce Releases Environmental Scan.

⁶¹ Manida Naebklang (2019), Report of the World Congress III against Sexual Exploitation of Children & Adolescents, https://ecpat.org/wp-content/uploads/legacy/ECPATWCIIIReport_FINAL.pdf.

⁶² Livingstone (2008), Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression, https://journals.sagepub.com/doi/10.1177/%201461444808089415%20(last%20visited%2016%20January%20 2020].

Instead, most victims choose to report it to the relevant online authorities or simply delete their accounts and block the offender."

Parents and educators should be aware that if they suspect online sexual abuse then the offender should be blocked and the communication retained as evidence. Parents should never view sexual images created by their child or other children. These materials should be turned over to law enforcement, and online abuse or exploitation of children should be reported to the appropriate authority. Parents should never pose as their child in order to "prove" abuse.

GUIDELINES FOR PARENTS, CARERS AND GUARDIANS

The safety tips draw on analysis of the data gathered and available research. This section of the report is intended to provide guidelines to parents, carers, and guardians (and educators in a separate list) to help them teach children and young people how to have a safe, positive and valuable experience while online.

Parents, carers, and guardians must consider the exact nature of sites, and their child's understanding of the dangers and the likelihood that the parent can reduce risks, before deciding which environment is right for their child.

The Internet has great potential as a means of empowering children and young people to help and find things out for themselves. Teaching positive and responsible forms of online behaviour is a key objective. Table 1 separates the issues into key areas for parents and guardians to consider.

Table 2: Key areas of consideration for parents, carers and guardians

	ō	V.:. A.: 6::.	
	#0N	consideration	Description
			Take an interest in what children and young people don't feel that their parents don't trust them. Filtering, monitoring and restricting access is what they are doing online, and have a conversation with them. It is important but it must happen alongside dialogue and discussion. When children and young people are spending time with others outside the home, they will have access to other (possibly unrestricted) devices, hence, the need for good communication – will they tell you if something went wrong? It is important not to overreact if children and young people tell you about something that has happened online. The important thing is that they have told you and reacting in the right way tends to make them feel confident that you can help them, and they will come back in the future.
Safety and security of your technology.	·	nave a discussion with your children. Try to do some online activities with them.	It can be helpful for children and young people to have an understanding of what the Internet is so that they have a better awareness of the Internet "space" in which their favourite platforms such as Instagram, Snapchat or YouTube exist.
			The Internet can often seem like an abstract place for children and young people and without some understanding of it, they can find it harder to frame the risks and recognise/visualise them. A possible analogy could be that of a large city which has lots of nice places and lovely people but also areas that you wouldn't visit as they could be risky. This will help children and young people to reflect on different "audiences" that they might encounter when they are online and how information can flow etc.
			Parents should take an interest in what their children do online and be prepared to share digital experiences with them as a way to foster trust and open up dialogue.
	5.	Identify the technology, devices and services	Starting with devices, identify all the devices in your home that are connected, including mobile phones, laptops, and tablets as well as smart televisions, gaming consoles, and fitness trackers in use across the family.
		household.	Identify the online services and apps that are being used across the family across all these devices.
		Install firewall and antivirus software on all devices.	Ensure that your devices have antivirus and malware protection installed and that it is kept up to date. Teach your children the basics of Internet security. E.g. is your operating system up to date, are you using the latest version of
	ю [;]	Consider whether filtering and blocking or monitoring programmes can help support and are suitable for your family.	
		- 1	

As soon as children and young people begin to use technology, discuss and establish a list of agreed rules. These rules should include when children and young people can use the Internet and how they should use it, as well as expectations of screen time. Digital Role Model - It is important that parents set the right example for their children. They are more likely to adopt the correct behaviours if these are being modelled by parents/carers. This might be extended to taking and sharing photos – consent should be sought before posting any images online. Consideration of parents' own use of the Internet and social media in relation to their child, such as sharing personal stories or photos about the child. Consider the child's privacy both now and in the future.	Children and young people need to be able to come and talk about whatever online (and offline) pressures and challenges they are facing. One way of enabling discussion is to use opportunities where stories about the Internet/online behaviour feature in the media. This will de-personalise the issue but will allow children and young people to express an opinion.	Have some understanding of how to ensure that children and young people are using apps and platforms as safely as possible, including making accounts private, being aware of age restrictions etc.	Make use of the tools that come with mobile devices such as Family Link or other parental control tools. Check to see if any products are sold or in-app purchases are included.	Try to have some understanding of the motivations of children and young people when they are online. Why are they using particular websites and services? What do different websites and services mean in terms of friendship groups, sense of identity, and belonging? This understanding will also you to better understand the social and emotional challenges children and young people may face, (which can sometimes result in riskybehaviour) and give them insights into how to build resilience.	Some countries have laws specifying a minimum age at which a company or website can ask a young person to provide personal information about themselves without first obtaining verifiable parental consent. This age of 'digital consent' typically ranges between 13 and 16. In some countries, it is considered to be good practice to require parental consent before asking younger persons for their personal data while in others, it is enshrined in law (see the GDPR article 8 for EU member states). Many websites that care for younger children will ask for parental consent before allowing a new user to join. Check each service for minimum age requirements.	Many devices, apps and services can be used to make purchases and carefully manage access to parental accounts with stored payment mechanisms and credit cards. It is important to keep your credit and debit cards secure, and not disclose your PIN numbers in order to prevent unauthorized access.	Know how to report problems on the platforms that your children are using and how to delete or make changes to profiles – as children get older, ensure that they know how to do this. Also, be aware of local reporting helplines.	Be aware that advertising can be inappropriate or misleading. Talk to your children about how they can report ads and take more control over what they see online. It is important to recognise that what children and young people see online can influence their views. Engage with them to help them to develop their online media literacy.
Agree on expectations as a family about using the Internet and personal devices, giving particular attention to issues of privacy, ageinappropriate websites, apps and games, bullying, screen time and stranger danger.	Also, ensure that there is a culture of support in the home so that children and young people feel able to seek support from parents/ carers.	Be aware of the online and mobile services	used by your children (i.e. social media,	websites, apps, games etc.) and have a good understanding of how children spend their time online.	Consider the age of digital consent	Control the use of credit cards and other payment mechanisms	Reporting	Advertising, misinformation and disinformation
4.			I	က်	Ö	7.	œ.	o.
Rules					Internet sites features review			

Children and young people need to understand that the online world is a reflection of the offline world – with good and bad experiences. It is important that children and young people feel confident that they can ask you for help and support if something has gone wrong as well as to be able to provide support for others online. Create a culture of support if something has gone wrong as well as to be able to understand the content they have posted and any online profile. Children and young people need to be able to recognise online risks -some are obvious but others less so – such as coercion, blackmail, and shaming. These mechanisms are all used by perpetrators and criminals. Children and young people also need to understand that online access comes with responsibility. They need to know that laws apply both online and offline and that they should behave in the right way.	As children and young people learn more about the online world, they may wish to meet up with people they don't know in real life, but whom they very formed a relationship with a relationship with a stranger of meeting up with a stranger they've been speaking with	The importance of Should post only information that you – and they – are comfortable with others seeing. They should not be sharing personal information. Personal information. Remind children and young people that they have an online reputation that needs to be managed. Once content has been shared it can be difficult to change/adapt.	Explain to your children that photographs can reveal a lot of personal information. Children and young people should and young people understand what without their consent. This should include parents taking and uploading images of their children. Equally, it is without that children and young people understand that sometimes it may be others, in their friend and family network who could let out information, so they should speak to their friends and families as well as educate them about oversharing. Encourage your children not to post photographs of themselves or their friends and their sweatshirts.
10.	[12.	
		-	
Children's education			

THE ROLE OF EDUCATORS

It is very important that educators do not make any assumption about what children and young people may or may not know about online safety issues, for example, an important role for educators is to teach children and young people about the importance of passwords, how to keep them safe and how to create a strong password: many teenagers share passwords with each other, and this is often seen as a sign of true friendship..

There is a good deal of debate about children and young people's privacy online and an evidence review carried out by the London School of Economics found that children and young people value their privacy and do engage in protective strategies, but they also appreciate the ability to be able to engage online. Similarly, the review found that parental enabling mediation was important in empowering children and young people, as it allowed them to experience some risk while learning independent protective behaviours. It also noted that "media literacy resources and training for parents, educators and child support workers should be considered because the evidence suggests that there are significant gaps in adults' knowledge of risks and protective strategies regarding children and young people's data and privacy online"⁶³.

Schools have the opportunity to transform education and help pupils to fulfil both their potential and to raise standards with ICTs. However, it is also important that children and young people learn how to be safe when they are using these new technologies, particularly more collaborative technologies such as social networking platforms and services, which are an essential aspect of productive and creative social learning. Children and young people are now easily able to create their own content and share this widely through social media platforms, most of which also allow live streaming.

Educators can help children and young people use technology wisely and safely:

- Make sure that the school has a set of robust policies and practices and that their effectiveness is reviewed and evaluated on a regular basis.
- Contributing to the development of digital skills and digital literacy by including digital citizenship
 education in their curricula. It is important to include social and emotional learning concepts
 within online safety education as these will support students' understanding and management of
 emotions to have healthy and respectful relationships, both online and offline.
- Ensuring that everyone is aware of the acceptable use policy (AUP) and its use. It is important to have an AUP, which should be age-appropriate.
- Check that the school's anti-bullying policy includes references to bullying over the Internet and
 via mobile phones or other devices and that there are effective sanctions in place for breaching
 the policy.
- Appointing an online safety coordinator.
- Making sure that the school network is safe and secure.
- Ensuring that an accredited Internet service provider is used.
- Using a filtering/monitoring product.
- Delivering online safety education to all children and young people and specifying where, how and when it will be delivered.

⁶³ Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri (2018), Children's Data and Privacy Online: Growing up in a Digital Age, http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/%20childrens-privacy-online/Evidence-review-final.pdf.

- Making sure that all staff (including support staff) have been adequately trained and that their training is updated on a regular basis.
- Having a single point of contact in the school and being able to collect and record online safety incidents will give the school a better picture of any issues or trends that need to be addressed.
- Ensuring that the management team and school governors have an adequate awareness of online safety in the school.
- Having a regular audit of all online safety measures.
- Appreciating the educational and psychological effects that the Internet and online technologies can have on children and young people.
- Children and young people's use of Internet technology has risen dramatically in recent years and has been accompanied by a growing concern about issues of online safety. Historically, there has been a recurring moral panic about the potential danger of communication technologies, and this has particularly been the case for young women. However, it has been argued that when such dangers are actually investigated, it appears that very often it is not the technology as such that is the culprit but more the increase in activity of the children and young people using the technology, more the anxieties about loss of parental control. Educators have been perceived to have a vital role in promoting and ensuring Internet safety. Parents across the world appear to believe that schools should have a central role in educating children and young people about the safe use of technology, but it is also clear from research that the main source of information on online issues for children and young people is from school and from parents⁶⁴. Further guidance on competencies that should be included in this type of education was identified as part of the Council of Europe Digital citizenship education project⁶⁵.
- Early approaches to online safety focused largely on technological solutions, such as the use of filtering software, but in recent years, there has been an increasing mobility of information technology and as a result, more traditional desktop computers are no longer the sole access point to the Internet. Increasing numbers of mobile phones, tablets, personal digital assistants and gaming consoles offer broadband connections and children and young people can access the Internet while at school, at home, in the library, at an Internet café, a fast-food outlet, a youth club or even travelling to school on public transport. Schools offer the opportunity to work on the Internet, collaboratively within a closed network or simply surrounded by other children and young people. Obvious initial measures include setting up effective security in the network. Children and young people may have personal devices that are not covered by network protection and this is why education, discussion and dialogue are crucial.
- Online safety policies need to be designed and implemented to involve a wide range of interest groups and stakeholders. These include:
 - school administration
 - District administration
 - support staff;
 - parents or caregivers;
 - local authority personnel;
 - where possible, Internet service providers and those who are providing Internet and broadband services to schools.

⁶⁴ Ofcom (2020), Children and Parents: Media Use and Attitudes Report 2019, https://www.ofcom.org.uk/data/assets/pdf_file/0024/190518/children-media-use-attitudes-2019-chart-pack.pdf.

⁶⁵ Council of Europe (2018), Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, Building a Europe for and with Children, https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/%2016808d881a%20.

As all of these groups have insights that can help set school policies, it is important that they are all consulted. However, simply having policies is not enough and everyone involved with children and young people should undertake active practices that help the staff to identify and achieve safe behaviour. By involving all these groups from the start, everyone should feel the relevance of such policies as well as their personal responsibility for making them real.

Creating a safe ICT learning environment has several important elements, which include the following:

- an infrastructure of whole-site awareness;
- responsibilities, policies, and procedures;
- an effective range of technological tools;
- a comprehensive e-safety education;
- programme for everyone in the establishment;
- a review process that continually monitors the effectiveness of the ICT learning environment.

These should all be embedded in existing child safety policies within the school, rather than being seen as something managed solely by an ICT team. It makes little sense to think of bullying over the Internet or via mobile phone as being something different from bullying in the offline world. However, this does not mean that technology cannot also be an important part of the solution through setting up:

- virus prevention and protection;
- monitoring systems to keep track of who downloaded what, when it was downloaded, and which computer was used;
- Filtering and content control to minimize inappropriate content via the school network.

The problems that arise in relation to new technologies do not apply to all children and young people, and when problems do arise, they depend on the age of the children and young people using these technologies. At the end of 2008, the Internet Safety Technical Taskforce in the United States of America produced a report on enhancing child safety and online technologies which provided a useful literature review of original, published research addressing online sexual solicitation, online harassment and bullying, and exposure to problematic content⁶⁶. Within this report it was noted that "There is some concern that the mainstream media amplifies these fears, rendering them disproportionate to the risks youth face." Over ten years later this is still the case with parents and educators being bombarded with attention grabbing headlines that are more likely to encourage adults to restrict access to online services than educate and empower children to use them safely.

This creates a danger that known risks will remain hidden and reduces the likelihood that society will address the factors that lead to them that can inadvertently be harmful. Media coverage of Internet mediated crimes against children and young people often seem to mirror the polarized positions of professionals and academics who work in the area, with the pendulum swinging between those who feel that there is a danger of distorting the threat posed to children and young people, and those for whom it appears that the threat has been underestimated.

However, there is concern that Internet mediated technology may leave some children and young people vulnerable and that educators, along with parents and guardians, have responsibilities with regard to this. The different ways in which children and young people may be victimized online include:

⁶⁶ ISTTF (2008), Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

- child solicitation or grooming;
- exposure to problematic or illegal materials;
- exposure to a medium that might foster harmful behaviour on the part of young people;
- Cyberbullying.

Informal education settings

Alongside school and home, children are likely to access the Internet and use services in non-formal settings such as youth clubs. The intertwining of online and offline life for children and young people means that those working with children in such settings are likely to have an influence on children's digital environment and their online safety, even if that is not their main focus. Therefore, all those working in more informal settings should have some understanding of the risks and opportunities and be able to support children appropriately or access the help and training that they require.

The key considerations and principles of the guidelines for educators also apply in such settings however there may be some contextual differences or additional considerations.

Managing devices, filtering, and communication

Support staff, volunteers, and children may be more likely to access services via their own devices in informal settings or systems to manage devices, and filtered content may be less available or less robust than in schools. Therefore, ensuring that practitioners and children understand how to secure and manage their own devices may require a greater focus in informal settings. Equally, with less sophisticated filtering options available, educators and children should not overly rely on them for protection.

Informal settings should still have robust and well-supported child protection policies and guidelines - however, in some settings educators or volunteers may not have access to an organisational device or email account in these settings. Extra consideration should, therefore, be given to the use of personal devices and if/how this is safely monitored/managed in policies and in practice.

Similarly, without access to 'education' technologies, equipment and support it may be more likely that mainstream social media and messaging services are used more frequently in informal settings than in schools. Extra consideration may, therefore, be needed in organisational policy, practice and training to identify if/how these are used and safely managed.

Training and support

Educators and volunteers working in informal settings may have less opportunity to engage with training, update their skills or access the range of support that may be available to educators in formal settings. How informal organisations find, deliver and fund training and support of this kind may need to be considered.

GUIDELINES FOR EDUCATORS

It is acknowledged that individual teachers/educators will not have control over some of the areas for consideration in Table 2 below, such as filtering and monitoring. It is expected that these actions would be taken by the school or the education setting.

Table 3: Key areas of consideration for educators

	SI. No#	Key Areas for consideration	Description
Safety and security of devices	1.	Ensure that all devices are secure and password-protected.	Teachers/instructors are as vulnerable as anyone else to cyber-attacks, malware, viruses and hacks. It is important that teachers should ensure that any device that they are using is properly protected (with strong passwords) and locked when not in use. (e.g. if a teacher needs to leave the classroom, then any device that they are using should be locked or the teacher should log off/sign out).
	2.	Install anti-virus software and firewalls.	Ensure that all devices have a firewall and anti-virus software installed and that this is kept up to date.
	3.	All schools should have a policy that governs where and how technology can be used within the school by different stakeholders and how child protection incidents are managed – including online.	Teachers need to ensure that they follow the policy regarding the use of mobile technology and other electronic devices. It is important that teachers model the correct behaviour when using devices. Schools should specify where and when mobile devices can be used.
	4.	Images of pupils.	Schools should have a policy which details whether photos of pupils can be taken. Are staff able to take photos for educational purposes? Has the relevant permission been granted by parents/ carers/pupils themselves? Ideally, the policy should state that personal devices should not be used for this purpose in order to safeguard both pupils and staff.
Filtering and monitoring	5.	Ensure that the Internet feed provided by the school is both filtered and monitored.	Pupils should not be able to access harmful or inappropriate content from the school IT systems. No filtering system can ever be 100 per cent effective and it is important to support these technical solutions with good teaching and learning as well as effective supervision. As a minimum, the filtering should prevent access to illegal content as well as content deemed to be inappropriate or harmful. As an example, the following categories of harmful content should be considered: Discrimination Hate speech Drug or substance abuse Extremism Pornography Piracy and copyright theft Self-harm or suicide content Extreme violence

	6.	Online reputation/digital footprint	Teachers need to be aware that what they say and do online can affect their reputation and also the reputation of the school/college. Teachers should always act in a professional manner online. Children also should be taught about the importance of online reputation and how to manage this effectively.
			There should always be a clear boundary between a teacher's personal life and their professional life – this includes online activity.
How to safely communicate		To recognise the importance of professional online communication	A school email address should always be used for any communication between staff and pupils or parents. Schools may wish to ensure communications policies or codes of conduct prohibit one-on-one communication and any communication without an education purpose or on non-school platforms.
professionally	7.	with pupils, parents and other stakeholders.	Ideally, personal devices should not be used to communicate with pupils or parents/carers.
			One-on-one digital communication should be avoided.
			If video-conferencing or remote learning is taking place, schools should be clear about the expectations of both staff and pupils. (e.g. thinking about where digital learning/communication is taking place i.e. not in a bedroom – have consideration of others who may be around in the home/classroom.)
Pupil behaviour and vulnerability online and the impact on safeguarding and wellbeing	8.	To understand the risks and benefits that pupils can be exposed to when they go online	Teachers need to have an understanding of what children and young people are doing when they go online and the risks and benefits that they can face.

CONCLUSION

The evolving digital landscape presents both opportunities and challenges for children and young people. While the internet offers avenues for learning, creativity, and social interaction, it also exposes them to various online risks. It is essential for parents, educators, and guardians to take proactive measures to ensure the online safety and well-being of the younger generation.

Cyberbullying and the creation of illegal child sexual abuse material are grave concerns that can lead to severe legal consequences. Beyond these risks, health-related issues such as excessive screen time and the potential infringement of personal rights, such as privacy and copyright, are prevalent in the digital realm.

Online safety campaigns are designed to change behavior and encourage responsible online practices, not only among children and young people but also within the broader community. These campaigns emphasize the importance of a collective effort to protect children online, involving parents, caregivers, educators, and various stakeholders.

Parents and guardians have a pivotal role to play in supporting their children's safe online experiences. By staying informed about potential online risks and engaging in open, age-appropriate discussions, they can empower children to navigate the digital world responsibly. Encouraging critical thinking, addressing peer pressure, and promoting balanced digital use are essential components of responsible online parenting.

Educators bear the responsibility of imparting crucial knowledge about online safety to children and young people. Digital citizenship education, which includes social and emotional learning, should be integrated into curricula. Schools should establish robust online safety policies, acceptable use policies, and anti-bullying measures, with designated online safety coordinators overseeing these efforts.

The digital world is not confined to formal educational settings; children also access the internet in informal environments like youth clubs. Educators and support staff in such settings should be equipped to understand online risks, manage personal devices, and address the use of mainstream social media and messaging services.

In this ever-evolving digital landscape, collaboration among parents, educators, caregivers, and various stakeholders is essential. By actively participating in children's online experiences, instilling responsible digital citizenship, and implementing robust policies and practices, we can create a safer and more secure online environment for the younger generation. Ultimately, the well-being of children and young people in the digital age relies on our collective commitment to fostering a culture of online safety and responsibility.

ACKNOWLEDGEMENTS

These guidelines have been adapted from the ITU's Guidelines for Parents and Educators 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 Parents and Educators 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





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 Parents and Educators 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 Parents and Educators. The localized guidelines were developed with the support from the International Telecommunication Union (ITU).

