

A White Paper

(Short Version)

9 February 2021

ChildSafeNet

unicef 



BACKGROUND

The increased access to digital technology, and usage of the internet and social media in Nepal, especially by children and young people, raises online safety concerns. Research studies on cyber safety, along with police and media reports, reveal that children and young people in Nepal are at high risk of online sexual abuse and exploitation, cyberbullying, phishing, identity theft and other forms of online harms. Risk is aggravated by inadequate response mechanisms and weak law enforcement, as well as a lack of awareness on the safer use of the internet among the majority of children, young people, parents, teachers and other stakeholders.

ChildSafeNet, in collaboration with UNICEF Nepal, prepared this white paper on protecting children and young people online, in order to assess the situation of children and young people's vulnerability to online harms, emerging threats, existing policies and plans, as well as response mechanisms and gaps. The white paper also provides key recommendations to duty-bearers and stakeholders to help make digital technologies safer for children and young people.

METHODOLOGY

The white paper incorporates the key outcomes of a systematic desktop review of over 120 relevant research reports, documents, policies, laws and international instruments. The white paper also includes the input and recommendations from six virtual workshops, and 21 stakeholders and child online protection experts.

OBJECTIVES

- To assess the magnitude, patterns, emerging trends and vulnerabilities related to online risks for children and young people
- To assess national policies, laws, response mechanisms and gaps related to online safety of children and young people
- To advocate with duty bearers for the development of appropriate policies and legal frameworks, as well as to strengthen response mechanisms
- To advocate for adequate investments from the government, private sector, civil society and parents to make the internet safer for children and young people

INTERNET USE IN NEPAL

In Nepal, 80.07 per cent of the population have access to broadband internet, and 58.83 per cent use mobile broadband internet services.¹ Due to the increased accessibility and affordability of smartphones and internet services, the majority of the internet users in Nepal access the internet on mobile devices. Likewise, 85.85 per cent of children and young people use the internet on mobile devices.²

In the past ten years, there has been a tremendous growth in internet users in Nepal. Only 2.65 per cent people in Nepal used the internet in 2010.³ According to a 2020 study conducted by ChildSafeNet and ECPAT Luxembourg with 500 children and young people in Kathmandu valley, 82.77 per cent of 13-17 year olds owned mobile devices/computers. Similarly, 97.66 per cent of participants aged 18-24 owned mobile phones/computers.⁴ Likewise, out of 11 million Facebook users in Nepal, four million are children and young people aged between 13 to 24 years old. According to the annual Nepal Media Survey of Sharecast Initiative, there were actually more people in rural areas using Facebook (88.6 per cent) than in the cities (87.5 per cent).⁵

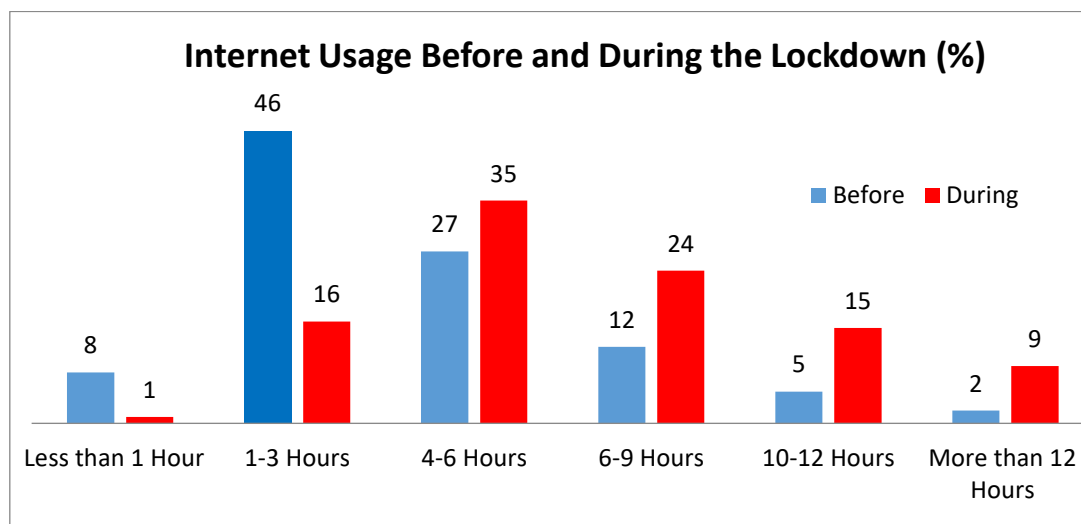


Figure 1: Internet use Before and During the COVID-19 Lockdown in Nepal (%)

As a result of the COVID-19 related lockdown, one in four children and young people (24 per cent) used the internet for more than ten hours a day, which is a notable increase from only 7 per cent who used the internet for more than ten hours a day before the lockdown.⁶ Moreover, entertainment (73.9 per cent), news and information (72.6 per cent), connecting with friends and relatives (63.2 per cent) and education (57.7 per cent) were cited as the main purposes of the internet by children and young people.⁷

¹ Nepal Telecommunications Authority, *Management Information System Report, Kartik, 2077 (October - November, 2020)* <https://nta.gov.np/wp-content/uploads/2021/01/MIS-Kartik-2077.pdf>

² ChildSafeNet and Unicef, *The Impacts of COVID-19 on Protection of Children and Young People Online – A Survey Report* (Unpublished manuscript)

³ Nepal Telecommunication Authority, *Management Information System Report, Jestha, 2067 (May 2010)* https://nta.gov.np/wp-content/uploads/2017/11/NTA_MIS_37.pdf

⁴ ChildSafeNet and ECPAT Luxembourg, 2020, *Rapid Assessment of Livestreaming of Sexual Exploitation and Abuse of Children and Young People* (Unpublished manuscript)

⁵ Dixit, Kunda, "Mobile Nepal Is Hooked on YouTube." *Nepali Times*, Himal Media Pvt Ltd, 5 Mar. 2020, www.nepalitimes.com/banner/mobile-nepal-is-hooked-on-youtube/.

⁶ ChildSafeNet and Unicef, *The Impacts of COVID-19 on Protection of Children and Young People Online – A Survey Report* (Unpublished manuscript)

⁷ ChildSafeNet and Unicef, *The Impacts of COVID-19 on Protection of Children and Young People Online – A Survey Report* (Unpublished manuscript)

MAGNITUDE OF THE PROBLEM

With greater numbers of children and young people using the internet and spending longer hours online, they are more exposed to online harms, such as, exposure to sexual content, sextortion, revenge porn, live streaming of sexual abuse and exploitation, cyberbullying, identity theft, phishing and other forms of cybercrimes. Generally, only a very few incidents get reported in Nepal, however, there has also been an increase in the total number of cybercrime reports.

According to The United Nations and the US Federal Bureau of Investigation, there are an estimated 750,000 predators online at any given moment.⁸ In Nepal, there were 172 reports of cybercrimes during the first month of the lockdown (March – April 2020), which constitutes 48.17 per cent of annual reports during the fiscal year BS 2075/76 (2018/2019).⁹ One in five girls aged 18-24 receives hate speech and sexual messages, photos or videos, whereas one in ten boys from the same age group receive such materials.¹⁰ Girls and boys as young as 12 years or below have also reported receiving such content.

According to a study conducted by ChildSafeNet in 2019, 41.15 per cent of children and young people said they had viewed online sexual content.¹¹ This was further substantiated by a ChildSafeNet and UNICEF survey conducted in 2020, which revealed that over 42 per cent of the children and young people participating in the survey had viewed online sexual content before.¹²

Although online abuse, exploitation and violence appear less serious than offline harms, these risks have serious consequences for children and young people. A sexual image or video posted on the internet can reach many people in a short time and can remain online almost forever. Therefore, the negative impact of such harms can be more serious and long-term.

Furthermore, as a result of online violence, children and young people can be susceptible to depression and self-harm. They could also experience abuse, exploitation and violence in the real world as a result of online relationships or harms, such as, sexual abuse or exploitation by child sex predators, or intimate partner violence and incidents of revenge porn between couples in romantic online relationships. Moreover, human traffickers are increasingly using social media to groom children and young women for the purpose of trafficking. Likewise, social media use has been identified as one of the main reasons behind child marriage in Nepal. A 2012 study by Save the Children, World Vision International, and Plan International¹³ attributed an increase in child marriages, in some areas of Nepal, to the increase in popularity of "love marriages" (for love and fulfilment of sexual desire)¹⁴ over traditional arranged marriages.

Most of the victims of online sexual abuse and exploitation hesitate to report and seek help due to a fear of being shamed, facing stigma and experiencing victim-blaming. Many families may feel that ignoring or hiding such incidents is the best response. As a result, many children and young people experiencing online harms suffer in silence.

⁸ *Webcam Child Sex Tourism, Becoming Sweetie: a Novel Approach to Stopping the Global Rise of Webcam Child Sex Tourism*. Terre Des Hommes Netherlands, 2013, p. 4

⁹ Central Cyber Bureau, Nepal Police, April 2020

¹⁰ *Ibid.*

¹¹ ChildSafeNet, *Living in the Digital Age*, 2019

¹² ChildSafeNet and Unicef, *The Impacts of COVID-19 on Protection of Children and Young People Online – A Survey Report* (Unpublished manuscript)

¹³ Plan, WVIN, Save the Children, Child Marriage in Nepal, Research Report, , 2012

<https://www.wvi.org/sites/default/files/Child%20Marriage%20in%20Nepal-%20Report.pdf>

¹⁴ Human Rights Watch, *Our Time to Sing and Play – Child Marriage in Nepal*, 2016 https://www.hrw.org/report/2016/09/08/our-time-sing-and-play/child-marriage-nepal#_ftn13

NATIONAL POLICIES

The Government of Nepal addresses the online protection of children and young people through its policies and directives. Nepal has the *Telecommunication Policy 2003*, *ICT Policy 2015*, *Online Child Safety Directives 2019*, *Digital Nepal Framework 2018*, *National Strategic Action Plan for Protection Cluster, 2016* and *Draft National Cyber Security Policy 2016* which can be referred to while discussing children's safety and protection from online abuse and exploitation. However, not all these instruments are explicitly focused on online child safety, except the *Online Child Safety Directives 2019*. However, these policies and directives need to be implemented effectively.

The Telecommunication Policy 2003 is mainly aimed towards increasing the access of the general public (from both rural and urban areas of Nepal) to telecommunication services, and for making arrangements to use appropriate information and communication technology for poverty alleviation and the development of rural areas.¹⁵ The Policy largely focuses on commercialization, liberalization and private sector participation in the telecommunications sector. It does not have any specific provisions related to the regulation of the internet, or ways to tackle the threats of online sexual abuse and exploitation that may arise after the increased and extended use of ICT throughout the country.

The Online Child Safety Directives 2019 was prepared and issued by the Nepal Telecommunications Authority (NTA). This is the first instrument in Nepal, prepared explicitly to address online safety of children. The Directives make it necessary for Internet Service Providers (ISPs) to provide information about the possible risks of the internet and on existing support mechanisms, to formulate and implement procedures for addressing complaints regarding child abuse content,¹⁶ to develop a framework for reporting abusive content or links, to set up a system to investigate the risk of children and adolescents, etc. However, these Directives are not comprehensive and are in need of revision.

The Digital Nepal Framework 2018 (Draft) affirms how the internet can be an important tool for fostering citizen and civil society participation, for the realization of development in every community, and for exercising human rights. The Nepal government has taken digital initiatives to make Nepal a prosperous country. Under the Digital Nepal framework, the government has identified eight sectors to intervene and develop, namely agriculture, health, education, urban infrastructure, energy, tourism, finance, and connectivity.¹⁷ However, the framework is silent about protecting children from online abuse and exploitation.

The National Strategic Action Plan for Protection Cluster, 2016 was prepared by the Ministry of Women, Children and Social Welfare, considering women, children, senior citizens and persons with disabilities as vulnerable populations to protect from natural disasters (such as earthquakes, flooding, landslides), human-caused disasters (such as armed conflict) and violations of human rights (such as, sexual and gender-based violence, kidnapping, child marriage, and many other child rights violations). This action plan was created for the overall protection of all vulnerable people, and does not on children or online safety.

The National Cyber Security Policy 2016 (Draft) is focused on data protection, national security, e-commerce, freedom of information, admissibility of electronic evidence, liability of Service Providers (SPs), child online protection and international cooperation. The Policy outlines the formation of a Child Online Protection Working Group (COPWG) to help identify areas of child online protection (such as technical protection measures, curriculums for school and information material for parents and guardians) that need attention. The COPWG will

¹⁵ No. 3 of the Telecommunication Policy 2003

¹⁶ No. 6 the Online Child Safety Directives 2019

¹⁷ Digital Nepal Framework 2018, (Draft) p. 2

ensure ISPs are obliged to provide, upon request of the user, restricted internet access that includes the ability to block content that is not appropriate for children. ISPs will be required to provide a “parental controls” function of the internet, if requested.

NATIONAL LAWS

The Constitution of Nepal (2015) has prohibited all forms of abuse and exploitation. Article 39 of the Constitution guarantees fundamental rights of children for the first time in the history of Nepal. Though the Constitution does not specifically mention protection from online abuse or cybercrimes, many articles in the document can still be exercised for the protection of children from abuse and exploitation.

The Act Relating to Children 2018 provides a legislative and institutional framework for the rights of the child.¹⁸ Among other outlawed conduct, the Child Act 2018 prohibits the exploitation of children in prostitution or other sexual work and covers some aspects of online child sexual exploitation. Article 66 clearly defines offences against children, including online sexual abuse and exploitation. Article 72 states the punishment for offenders is a fine up to eighty thousand rupees, and four years of imprisonment, depending on the type and severity of the crime.

The Electronic Transaction Act BS 2063 (2008), Article 47 states that any person who publishes or displays materials through electronic media, including images and videos, that is of a legally/morally prohibited sexual nature, or against decent behaviour, shall be liable to a fine of Rs. 100,000 or five years of imprisonment or both. Article 55 of the Act has provisions to prosecute offenders, committing crimes from foreign countries. In 2015, Section 58(a) was added in the Act to provide compensation to victims.

Criminal Code Act 2074 (2017)¹⁹ penalises cyber-crimes as specified in Article 300, which states that harassing, threatening, insulting and improper behaviour online carries a sentence of one year of imprisonment, or a fine of Rs. 50,000, or both. Similarly, Article 307 of the Act addresses the issue of defamation. If an online platform is used to defame or insult a person, an additional sentence of one year of imprisonment and a fine of Rs. 10,000 is added to the original sentence. Article 307 (2) also has a provision for the compensation of victims, which includes the costs borne while taking legal action. Article 308 of the code states that a complaint has to be made within 3 months of a person being aware that the crime has been committed.

INTERNATIONAL INSTRUMENTS

Some legal instruments have been developed at the international and regional levels to deal with online abuse and exploitation of children.

Convention on Cybercrime (Budapest Convention) 2001²⁰ is the most comprehensive legal document covering online child abuse and exploitation. This is the first international treaty seeking to address internet related crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. The Budapest Convention, adopted in 2001 came to force in 2004. Among others, the Convention defines illegal access, illegal interception, data interference, system interference, misuse of devices,

¹⁸ *Briefing Paper: Sexual Exploitation of Children in Nepal*. ECPAT International, January 2020, <https://www.ecpat.org/wp-content/uploads/2020/01/ECPAT-Briefing-Paper-on-the-Sexual-Exploitation-of-Children-in-Nepal-2020-ENG.pdf>

¹⁹ Government of Nepal, Nepal Law Commission. “Criminal Code Act, 2074 (2017).”

²⁰ https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest/7_conv_budapest_en.pdf

computer-related forgery, computer-related fraud and offences related to "child pornography". Nepal is not a party to this Convention. However, as a non-Council of Europe country, Nepal can accede to this convention and strengthen its domestic legal provisions for the protection of children of children online.

The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (also known as The Lanzarote Convention),²¹ adopted in 2007 by the Council of Europe, is a major step in the prevention of sexual offences against children, the prosecution of perpetrators and the protection of child victims.²² This is the first time that an international treaty has identified and criminalised the offence of sexual abuse, such as, causing or coercing or facilitating children to engage in pornographic activities. However, the Lanzarote Convention does not specifically define or criminalise all forms of sexual exploitation of children, including sextortion, online child sexual abuse materials. According to the Article 20 (1) and (3), parties have the right to not to criminalise virtual "child pornography".²³ Nepal is not a party to the Lanzarote Convention, but it can accede to it as a non-Council of Europe country.

The UN Convention on the Rights of the Child (CRC), ratified by Nepal in 1990, has clear provisions to protect children from sexual abuse and exploitation. It addresses the issue of child sexual abuse materials (CSAMs) through appropriate actions by the State parties to protect children from sexual exploitation of children through pornographic performances and materials (Article 34).

The Optional Protocol to the UN Convention on the Rights of the Child on the Sale of Children Child Prostitution and Child Pornography (OPSC)²⁴ – The Government of Nepal ratified the Optional Protocol to the United Nations Convention on the Rights of the Child in 2006.²⁵ The OPSC criminalizes the act of offering, delivering or accepting by whatever means, a child for the purpose of sexual exploitation (Article 3(1)a).

The ILO Convention 182 concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour²⁶ criminalizes the use, procuring or offering of a child for [...] pornographic performances (Article 3(b)).

RESPONSE MECHANISMS AND SUPPORT SYSTEMS

Children and young people experiencing online harms have inadequate, or no access to support systems in Nepal. There is a lack of institutional response mechanism for legal, psychosocial, medical and technical support. Most parents and duty bearers also do not have the necessary knowledge or awareness on the severity of online harms against children and young people in order to be able to address them effectively. This was found to be evident through a study conducted by ECPAT among 4,778 parents of Nepal, among which 40.6 per cent did not see any probable online risks for their children, and 26 per cent did not know about such risks.

It is important to provide treatment for victims who display sexually abusive behaviours online, and such treatment should follow the same approaches used for those who commit sexually harmful acts offline. There should also be a comprehensive assessment of the child and how to intervene through rehabilitation and counselling, an assessment of the child's development

²¹ <https://rm.coe.int/1680084822>

²² <https://rm.coe.int/1680471b5a>

²³ https://www.ecpat.org/wp-content/uploads/2016/04/Legal%20Factsheet%20-%20Lanzarote%20Convention_0.pdf

²⁴ *Livestreaming of child sexual abuse in real-time*, ECPAT International.

²⁵ <https://www.ohchr.org/EN/HRBodies/CRC/CRC30Pledges/Pages/Nepal.aspx>

²⁶ *Livestreaming of child sexual abuse in real-time*, ECPAT International.

and motivation, and the active involvement of parents throughout the whole process. Similarly, criminal investigations should adhere to child sensitive approaches by taking into account the profound difficulties often experienced by children and young people in disclosing online abuse.²⁷

ORGANIZATIONS WORKING ON ONLINE SAFETY OF CHILDREN AND YOUNG PEOPLE AND THEIR INITIATIVES

SN	Organisation	Key Initiatives
1	ChildSafeNet www.childsafenet.org	<p>ChildSafeNet is the only organisation in Nepal with the sole mission to make the internet safer for children and young people, and to protect them from online abuse, exploitation and violence. Research, training, awareness-raising and advocacy are main programme activities of ChildSafeNet.</p> <p>The organisation has conducted a number of research studies and surveys on online protection of children and young people, including a research studies on children and young people's online behaviour and risks (2018-19), live streaming of sexual abuse and exploitation of children and young people (2020) and a survey on COVID-19 and its impacts to the protection of children and young people online (2020).</p> <p>ChildSafeNet is working with UNICEF Nepal to develop a white paper and has conducted desktop review of over 120 documents (research reports, policies, laws, technical papers and other relevant documents). The organisation has also developed a technical note on COVID-19 and the protection of children and young people online, four toolkits (for police, lawyers, psychosocial service providers and parents), a cyber safety booklet and a detailed FAQ.</p> <p>ChildSafeNet has developed offline and online training modules on cyber safety. Every year, the organisation conducts cyber safety training of trainers and has thus far produced more than 60 trainers. ChildSafeNet's training programmes have benefitted more than 4,000 children, young people and parents.</p> <p>ChildSafeNet has produced video PSAs, digital posters, articles and blogs on cyber safety to raise awareness.</p> <p>ChildSafeNet has the national coordinator of Safer Internet Day (www.saferinternetday.org) in Nepal, since it was first initiated in 2019.</p>
2	CWIN Nepal www.cwin.org.np	<p>CWIN Nepal is a leading child rights organisation of Nepal. They conducted a research study on the online safety of children in Nepal in 2008.</p>

²⁷ *Child Safety Online, Global Challenges and Strategies*, UNICEF Innocenti Research Centre, Italy, 2011, available at https://www.unicef.org/protection/files/Child_Safety_online_-_Global_challenges_and_strategies_FINAL_1Dec.pdf

		CWIN has produced video and print awareness materials on internet safety. The organisation has also conducted a research study on online safety of children in 2020.
3	ECPAT Luxembourg (www.ecpat.lu)	<p>ECPAT Luxembourg has collaborated with Voice of Children to raise awareness on cyber safety, and has conducted a research study on online sexual exploitation of children in 2017.</p> <p>ECPAT has also conducted a research study on online safety in 2019. The organisation collaborated with ChildSafeNet to conduct a rapid assessment report and research study on livestreaming of sexual abuse and exploitation of children and young people in Nepal (2020).</p> <p>ECPAT Luxembourg has provided support to the Central Cyber Bureau of Nepal Police on awareness raising.</p>
4	Voice of Children (www.voiceofchildren.org.np)	<p>Voice of Children raises awareness on online child sexual abuse through school orientations, community orientations, social media, etc. Voice of Children also conducts capacity building workshops and training for stakeholder groups, such as teachers, social workers, health workers, hoteliers and journalists.</p> <p>The organisation publishes IEC materials on online sexual abuse, has broadcast a radio program and TV program, and formed a radio listener's club, to raise awareness on online sexual abuse.</p> <p>Voice of Children provides support to children and young people who have been affected by online sexual abuse through means such as providing shelter, nutrition, education, psychosocial support, legal assistance, livelihood support, etc.</p>
5	SathSath (www.sathsath.org)	<p>Sathsath has conducted cyber safety awareness activities, with a focus on sexual abuse and exploitation of boys.</p> <p>Sathsath has produced IEC materials on cyber safety.</p>
6	Srijansheel Samaj Nepal	Srijansheel Samaj Nepal has conducted cyber safety training for children and young people, in collaboration with UNICEF Nepal.
7	UNICEF (www.unicef.org)	<p>UNICEF Nepal has conducted cyber safety awareness activities under its Net4Good programme. The organisation has produced video and print IEC materials, and provides support to conducting cyber safety training.</p> <p>UNICEF has partnered with ChildSafeNet to develop a white paper on cyber safety for children and young people, and to conduct a desktop study of research studies, policies, laws, international instruments, technical papers and other relevant documents. Under ChildSafeNet's initiatives, UNICEF Nepal has supported the development of toolkits and other resources.</p>

8	Forum For Digital Equality/Child Safety Initiative (www.childsafety.org.np)	<p>Forum For Digital Equality/Child Safety Initiative has set up a complaint portal for cybercrimes related to children and young people. The organisation also conducts awareness-raising activities on online risks for children and young people.</p> <p>Additionally, Forum For Digital Equality/Child Safety provides legal aid and psychosocial support to children and young people who are victims of online crimes, gives courses on digital parenting and capacity building for stakeholders, provides technical assistance regarding issues related to cybercrimes, and conducts research into online safety for children and young people.</p>
9	LOOM (https://taannepal.org.np/)	<p>LOOM has conducted a workshop with young women with digital security as a key component. The workshop was conducted online for young women from Sunsari and Udayapur districts. The workshop focused on how young women can use the internet safely, guiding participants to protect their personal data through various techniques.</p> <p>LOOM has also published a digital security handbook for young women, and publications on online violence against women.</p>

GAPS

Knowledgebase: Since very few studies have been conducted in Nepal on online risks and safety of children and young people, there is a limited knowledgebase on the problem, its magnitude, patterns, vulnerability and impacts. In 2008, Child Workers in Nepal Concerned Centre (CWIN) conducted a study on online risks for children.²⁸ Another similar study was conducted nine years later in 2017 by ECPAT Luxembourg and Voice of Children.²⁹ Subsequently, ECPAT Luxembourg conducted a study in 2019 on internet safety.³⁰ Likewise, ChildSafeNet conducted a study on children and young people's online risks and behaviour in 2019.³¹ In order to fill the thematic knowledge gap, ChildSafeNet and ECPAT Luxembourg conducted a study on live streaming of sexual abuse and exploitation of children in 2020.³² Furthermore, in April 2020, UNICEF and ChildSafeNet conducted a study on the impacts of the COVID-19 pandemic on online safety of children and young people.³³ Although there is basic information on online safety, there is not much knowledge on the different manifestations of online harms against children.

Awareness: The lack of understanding on the manifestations and magnitude of online abuse and exploitation of children and young people is a deterrent in tackling online harms. Many children also do not realise that they have faced online harms, particularly when they are involved in producing and sharing sexual content with their friends, partners or with strangers online. Furthermore, very few children, young people and parents are aware of online safety.

²⁸ Child Workers in Nepal Concerned Centre (CWIN) & Save the Children Sweden Regional Office, *Study on the Internet Use by Children in Nepal*, Kathmandu, 2008

²⁹ ECPAT Luxembourg and Voice of Children, *Assessing and Understanding the Risk: Sexual Exploitation of Children Online in Nepal*, 2017

³⁰ ECPAT Luxembourg, *Internet Safety and Risks of New Technologies to Children in Nepal*, 2019

³¹ ChildSafeNet, *Living in the Digital Age*, 2019

³² ChildSafeNet and ECPAT Luxembourg, 2020, *Rapid Assessment of Livestreaming of Sexual Exploitation and Abuse of Children and Young People* (Unpublished manuscript)

³³ ChildSafeNet and Unicef, *The Impacts of COVID-19 on Protection of Children and Young People Online – A Survey Report* (Unpublished manuscript)

Law Enforcement: Article 60 of the Electronic Transactions Act (2008) has a provision for the establishment of a Tribunal for the purpose of hearing cases on crimes committed through electronic means, but as of August 2020, such a Tribunal has still not been established, and the Kathmandu District Court remains the only court designated to hear such cases.

Policies: Although there are policies and directives for online protection of children and young people, there is a gap in implementation. Some policies and directives may also need amendment, as mentioned above under the "Policies" section. Additionally, due to a lack of concrete definitions regarding cybercrimes in existing policies, there is an ambiguity to how certain cybercrimes are considered and handled. As a result, punishments often vary on a case-by-case basis.

Response Mechanisms and Support Services: Children and young people who experience online abuse, exploitation and violence have very little or no access to support services. There are gaps in provisions of the following support services:

Medical Support: There is confusion among many about the medical support needed to victims and survivors of online exploitation. There has been evidence that a lot of offline crimes have online components,³⁴ and crimes committed offline are, thus, also often online. Victims and survivors may need both physical and mental health support.

Psychosocial Support: Most victims and survivors of online abuse go through mental distress and trauma, often leading to self-harm. They need psychosocial support to build their self-confidence and to be brought back to their normal life routine. There is also the question of providing psychosocial support to troubled children and young people who are accused or guilty of committing online crimes, as there may be a deeper psychological reasoning for why they commit such offensive acts.

Legal Aid Support: Victims and survivors should be provided free legal support from the time of first lodging a First Information Report (FIR), to the final hearing in court. They may not know the legal process and they may not be able to afford the legal fees.

Technical Support: Though it is the responsibility of investigators to collect evidence and have the technical knowledge necessary to do so, victims and survivors may also need to be provided with information related to texts, photos, videos or similar proofs. They may not be able to provide the required information or facts due to a lack of technical knowledge. Thus, technical support is an essential component of victim support in the context of online abuse.

RECOMMENDATIONS (FOR ADVOCACY & AWARENESS RAISING)

Government

- Develop, amend and implement policies to protect children and young people online and promote safer use of the internet.

Designate one government body to oversee and coordinate online safety of children and young people.

³⁴ Protecting yourself from the latest internet sex crime, Michigan State University, April 2020. Available at: <https://phys.org/news/2020-04-latest-internet-sex-crime.html>

- Online safety of children and young people need to be strictly prioritized by the Government. Government should allocate adequate financial resources and develop necessary infrastructures in schools to educate children on online safety.
- Develop and strengthen institutional structures at the federal, provincial and local levels.
- Formulate and adopt comprehensive laws addressing cybercrimes for effective legal protection of children and young people, defining terms like child sexual abuse materials, online sexual abuse and exploitation of children, cyber grooming, solicitation of children online for sexual purposes, 'sexting', 'sextortion', live streaming of sexual abuse and exploitation, cyberbullying, hate speech, right to privacy online, identity theft, phishing and other new forms or online harms.
- Develop a uniform system of reporting, complaint handling, and protection for victims and witnesses of online sexual exploitation throughout Nepal.³⁵
- Develop a multi-agency collaboration platform and monitoring/supervisory mechanism.
- Incorporate age-appropriate internet safety education in school and college curricula, starting from early years.
- Strengthen inter-generational cyber safety education strategies which can be helpful in increasing understanding between different generations about the safe use of technology.³⁶
- Facilitate effective initiatives to make children and young people aware of the positive aspects of using the internet. Make the internet accessible and affordable throughout the country and reduce the digital divide so that all children can benefit from having access to the internet, including but not limited, for education, information, entertainment and communication.
- Engage, work and develop partnerships with civil societies, private sector, development sector workers, Internet Service Providers and mobile operators to plan and implement internet ethics.

Police

- Strengthen law enforcement and create an effective system to report online abuse and exploitation of children and young people.
- Enhance capacities of police officials on dealing with cases related to cyber-crimes against children and young people throughout the country.
- Facilitate reporting of cases of cyber-crimes against children and young people using child-friendly procedures.
- Enhance knowledge and skills of police officials on child-friendly investigation procedure.

³⁵ Kapil Aryal, *Internet Safety and Risks of New Technologies to Children in Nepal*, ECPAT Luxemburg, 2019.

³⁶ *Addressing the Cyber Safety Challenge: from risk to resilience*, 2014, p. 11, available at <https://core.ac.uk/download/pdf/30674272.pdf>

- Ensure that children in contact with the law are treated with dignity as per the established standards of the juvenile justice system.
- Ensure that child victims and their witnesses are protected.
- Strengthen the technical capacity to investigate online sexual abuse and exploitation of children and young people.
- Expand the “Cybercrime Offices” in the Nepal Police to all districts of Nepal, not just Kathmandu.

Nepal Telecommunications Authority and ICT Sector

- Follow the United Nations Guiding Principles on Business and Human Rights and call on businesses to meet responsibilities to respect children’s rights by avoiding any adverse impacts linked to operations, products or services.³⁷
- Effectively filter, block and report child sexual abuse and exploitation materials online.
- Take initiative to foster approaches which can be used to automatically limit information disclosure on Online Social Networks by providing a list of reliable friends with whom the user can securely share their private posts.
- Restrict children's access to adult sites and streaming of sexually explicit content, including child sexual abuse and exploitation materials.
- Ensure that websites/content that harm children and young people are monitored. Develop techniques like machine learning (ML) and artificial intelligence (AI) for detection and prevention of online child abuse materials and incidences, block keywords used to access inappropriate websites based on blacklisted search terms. Similar methods like IP blocking, Domain Name System (DNS) filtering, and Uniform Resource Locator (URL) blocking should be implemented.
- ISPs should provide information to parents on parental control applications to help them monitor online activities/behaviours of their children.
- ISPs and telecommunications operators can send push-notifications and bulk messages to raise online safety awareness.

Schools and Colleges

- Develop school/college-wide cyber safety policies and implement them effectively.
- Launch internet safety training and internet literacy training for teachers and parents.
- Provide awareness on online safety and risks through drama, poetry, songs and provide more practical lessons to students.

³⁷ *Children’s Right and the Internet: From Guidelines to Practice, Articles from the Guardian Sustainable Business Child Rights Hub*, UNICEF, 2016, p.7, available at https://www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainable_Business_English.pdf

- Educate parents and teachers on parental control systems in their mobile; laptops, computer and other similar devices.
- Schools and colleges should educate children about the technical skills to better equip themselves from online risks while also providing a broader understanding on online safety.
- Introduce e-learning concepts to students and make their online classes safer.
- Develop a complaint lodging mechanism in schools and colleges if children and young people experience any forms of online bullying, exploitation, grooming, etc.
- Provide psycho-social counselling to students who may have a hard time talking/sharing their negative experiences to parents and teachers. Counselling can be a good medium to communicate freely without any fear of judgment.
- Encourage positive behaviours online, filter and monitor content on school/college computers, used by children and young people.

Civil Society Organizations/Institutions

- Design and implement programmes to address online and offline sexual abuse and exploitation and how they can be inter-related.
- Develop and use standardized cyber safety training modules to ensure consistency and accuracy. Conduct virtual training when schools and colleges are closed due to the COVID-19 pandemic.
- Conduct cyber safety training for children and young people, as well as parents.
- Develop capacities of social workers and service providers for responding to online sexual abuse and exploitation.
- Conduct campaigns to raise awareness on the safer use of the internet among parents, caregivers and schools.
- Promote awareness on reporting online crimes against children and young people.
- Work together to establish effective reporting mechanisms – e.g., hotlines, report abuse functions, and online supports – to provide support services to children and young people facing risks online.
- Operate child helplines and support services for children and young people.
- Create age-appropriate, child-friendly awareness materials that are easily accessible e.g. short videos, comics, social media posts, etc.
- Take in consideration of specific vulnerabilities, e.g., language barrier of certain groups, gender differences, members of the LGBTQI+ community, children with disabilities etc., as certain groups are more vulnerable to online abuse, or are disregarded as victims or survivors. When designing programmes, include representatives of beneficiary groups, such as, children and young people from the LGBTQI+ community, from different ethnic

and language groups, with different abilities (disabilities), by following ethical guidelines and ensuring the protection and respect of children's rights.

- Advocate with the government, private sector, media, schools and tech companies.
- NGOs running child protection helplines and other services should keep their services running and on high alert. These services should be considered as essential social services, particularly during the COVID-19 pandemic.
- Establish a national research working group where researchers can co-operate and support each other for more efficient and comprehensive results for data collection, data verification, reporting and dissemination.
- Conduct thematic studies, such as, peer sexual abuse and exploitation, vulnerabilities among different age groups as well as gender and minority groups.

UN, INGOs, Regional and International Organizations

- Provide technical assistance for effective programme implementation.
- Assist in developing policies and systems for the protection of children and young people online.
- Facilitate inter-agency coordination and collaboration.
- Provide support to civil society organisations in protecting children and young people online, for research studies, awareness raising, capacity building, support services and advocacy.

Media

- Conduct media literacy programs and online safety educational campaigns for children and young people. These efforts should be accompanied by public awareness campaigns to better inform parents about parental control tools for monitoring purposes.³⁸
- Mainstream and online media (e.g., online news portals, YouTube channels, etc.) to convey positive messages and create awareness on online safety.

Parents/Guardians

- Learn about online risks and children and young people's vulnerability to online sexual abuse and exploitation. Parents should proactively and regularly access cyber-safety resources designed for them to become familiar with emerging technologies and online trends.
- Spend one-to-one time with children and help them to use the internet safely. Teach children about online dangers. Share measures on safe internet use, including making online accounts private, avoiding providing personal information to unknown sites/people

³⁸ Thierer, A., *Rep. Bean's "Safer Net Act": An Education-Based Approach to Online Child Safety*, Periodic Commentaries on the Policy Debate, The Progress & Freedom Foundation, 2007, p. 2.

online, frequently changing passwords, and being careful while downloading online content.

- Provide information to children on age-appropriate websites and online content.
- Encourage children to fact check information online.
- Monitor children's online activities and who they are communicating with online. Be alert to signs of distress. If children appear withdrawn, upset, secretive or obsessed with their online activities, it could be an indication for an issue they are facing online (e.g., online sexual abuse and exploitation and cyberbullying).
- Understand the needs, interests and curiosity of children while making reasonable rules within the home space, such as limiting screen time to 3-4 hours a day.
- Encourage children to talk and initiate free conversations if they ever face risks online. Listen to children without judgment and guide them towards a better solution, rather than blaming them. Communicate openly with children. Be patient, make sure they feel comfortable enough to speak with parents.
- Learn about reporting online abuse cases to the police, preserving evidence, as well as reporting and blocking abusers on social media platforms and receiving support services.

Children and Young People

- Learn about internet safety.
- Avoid interacting with online strangers or people not known very well to you. Do not accept friend requests from strangers or people not known very well to you.
- Do not share private information publicly online.
- Check and set privacy settings on websites and platforms regularly accessed.
- Block anyone who makes you uncomfortable.
- Tell parents, guardians or trusted adult/s about any bad experiences you have online
- Do not visit untrusted sites or use anonymous video chat and live streaming apps.
- Do not take, store or share your own, or others', nude or sexual photos and videos. Do not share private pictures, videos, or other self-identifying information publicly or with strangers or the people not known very well to you.
- Spend time away from your devices and disconnect from the internet. It is very important to maintain a healthy balance between online and offline time.
- Be mindful while using the internet. Treat other people with respect. Do not take advantage of other people's trust and harm them, including while using the internet. Respect other people's rights to privacy and confidentiality.

- Know where to report online abuse and exploitation and the organisations and people where you can get help.

CONCLUSION

The considerable influence of the internet on our lives shall continue to grow and evolve. High internet penetration and the low cost of digital devices in Nepal has benefitted children and young people, however, has also exposed them to various online harms. Cases of online crimes committed against children and young people are continuously increasing. However, Nepal lacks adequate legislative, administrative, infrastructural, and technological and human resources to tackle these crimes.

While there are numerous benefits of internet use – connection, e-learning and entertainment – during the lockdown, it comes with a host of potential risks as well. Since more people are online than usual, the chances of children encountering predators online has increased, as has the chances of being exposed to age-inappropriate content or being cyberbullied. Children and young people are also more likely to display increased risk-taking behaviour, which can put their privacy at risk. Other aspects of the internet children are susceptible to include the risks related to livestreaming, and the risk of developing a gaming or internet addiction.

Staying at home does not ensure children’s safety from external dangers drawn in via the internet. It is important to teach children safe online practices and increase their digital literacy to make sure they understand both the benefits and the risks of the internet, thus ensuring their long-term safety.

Government, civil society organisations, UN agencies, international organisations, schools, ISPs, ICT companies, parents, guardians, caregivers, and children and young people themselves have important roles in making the internet safer.

Strengthening collaboration and cooperation among different stakeholders is the foundation of creating a safe and protected online space for children and young people. The Government, law makers, the police, private sector, ISPs, tech companies, schools, colleges and parents have a responsibility in ensuring and protecting the rights of children and young people online. Given that technology will continue to become more integrated into our everyday lives, it is important that cyber safety strategies are flexible and adaptable enough to respond to new opportunities and challenges.

Project Team

Anil Raghuvanshi

Team Leader

Kapil Aryal

Content Writer

Neha Gauchan

Research Officer

Darshana Gauchan, Ristha Shrestha, Swasti Karmacharya, Aashrika Chaudhary

Research Assistants