NEPAL'S DIGITAL GENERATION:

CHALLENGES AND SOLUTIONS FOR CHILD ONLINE PROTECTION

A Situation Paper

2024

CONTENTS

LIST OF ABBREVIATIONS

CSAM	Child Sexual Abuse Material
CSEM	Child Sexual Exploitation Material
DNS	Domain Name System
ETA	Electronic Transactions Act
GBV	Gender-Based Violence
ICT	Information and Communication Technology
INGO	International Non-Governmental Organization
IPV	Intimate Partner Violence
ISP	Internet Service Provider
IT	Information Technology
LGBTQIA+	Lesbian, Gay, Bisexual, Transgender, Queer, Intersex and Asexual
MNR	Model National Response
NGO	Non-Governmental Organization
NTA	Nepal Telecommunications Authority
OECD	Organization for Economic Co-operation and Development
UNICEF	United Nations Children's Fund
URL	Uniform Resource Locator
WYESHR	Women Youth Empowerment in Social Service and Human Rights

FOREWORD

In the digital age, where the internet has become an integral part of people's lives, ensuring the safety of children and young people online has emerged as a critical concern. Nepal, like many other countries, is experiencing a surge in internet usage among its youth population. However, with increased connectivity comes heightened risk of online abuse, exploitation and exposure to harmful content.
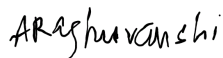
This situation paper, a collaborative effort between UNICEF Nepal Country Office and ChildSafeNet, endeavours to shed light on the prevalent online risks and challenges faced by children and young people in Nepal. Through a thorough examination of over 160 research reports and documents, supplemented by insights from 20 experts and stakeholders in child online protection, this paper presents key findings that underscore the urgent need for action. Among the findings is the significant increase in internet usage among Nepalese children and young people. This increased connectivity has also led to a rise in risky online behaviours, exposing them to potential harm. Furthermore, the paper highlights the inadequacy of legislative, administrative, infrastructural, technological and human resources in Nepal to effectively address cybercrimes against children.

In response to these findings, the situation paper puts forth a comprehensive set of proposed recommendations aimed at various stakeholders. To the government and policymakers, it advocates for the enactment of comprehensive ICT laws and the establishment of internet ethics to ensure a safer online environment. The paper also calls upon the Nepal Telecommunications Authority and the ICT sector to uphold human rights standards and implement measures to monitor and control harmful online content. Educational institutions are urged to integrate online literacy and safety courses into their curricula, while media outlets are encouraged to conduct media literacy programmes and implement ethical reporting guidelines. NGOs and INGOs are called upon to collaborate on efficient reporting mechanisms and continuous research efforts to combat cybercrimes against children.

We believe this paper will serve as a powerful programming and advocacy tool to catalyze meaningful and timely actions for the development of appropriate policies and legal frameworks, as well as to strengthen response mechanisms and to advocate for adequate investments from the government, private sector, civil society and parents to make the internet safer for children and young people. Ultimately, this situation paper underscores the importance of collaborative efforts and cooperation among all stakeholders in laying the foundation for safe and secure internet use. As Nepal and other developing countries continue to navigate the challenges and opportunities presented by the digital revolution, safeguarding children and young people online must remain a collective priority.

This paper serves as a call for action to protect children, the most vulnerable members of our society in the digital age. It is our collective responsibility to ensure that children and young people can harness the transformative power of the internet without falling victim to its dangers.

Anil Raghuvanshi
Founder and President
ChildSafeNet

Alice Akunga
Representative
UNICEF Nepal

EXECUTIVE SUMMARY

Background

The growing access to and adoption of the internet and social media in Nepal has expanded the accessibility of digital platforms for children and young people. This surge raises serious concerns regarding their online safety. Studies indicate that issues such as unsafe internet and social media usage, breaches of social media policies, inadequate response mechanisms, and a lack of information on safe internet usage are commonly encountered by children, parents, teachers and other stakeholders.

There is a limited knowledge base on how children and young people are using the internet for study, information, communication and entertainment. At the same time – and despite some research studies that have been conducted on online risks and child online safety in Nepal – there is also a limited knowledge base on the trends, patterns, gravity, impacts and magnitude of online abuse, exploitation and violence against children and young people in Nepal.

UNICEF Nepal Country Office and ChildSafeNet developed this situation paper to identify the knowledge gap on the online risks and challenges for children and young people. Besides reviewing the current state of children's and young people's internet safety in Nepal, this situation paper proposes a set of recommendations to the duty-bearers and service providers for action to protect children and young people in the digital age.

This situation paper is intended for a wide array of stakeholders, including the government, policymakers, police, judicial bodies, the Nepal Telecommunications Authority (NTA), the information and communication technology (ICT) industry, educational institutions (schools as well as colleges), journalists, United Nations agencies, international and national non-governmental organizations (I/NGOs), as well as parents, guardians and children's caretakers.

Methodology

This situation paper has been prepared by ChildSafeNet in close collaboration with UNICEF Nepal, incorporating the key outcomes from a systematic desktop review of over 160 research reports and documents. The paper also includes the input and recommendations of over 20 experts and stakeholders in child online protection, as well as input collected from participants in six virtual workshops organized by ChildSafeNet.

Key findings

1. The internet's impact on people's lives is already significant, and its usage and influence is expected to continue to grow.
2. Nepal has experienced a notable increase in internet usage.
3. A growing number of children and young people are actively using the internet in Nepal.
4. Widespread instances of children and young people engaging in risky internet behaviour have been identified.
5. The extended time spent online by children and young people exposes them to a higher risk of online abuse and exploitation.

6. While Nepal stands to benefit from increased internet connectivity, there are associated risks and hazards that need immediate attention.

7. Nepal lacks essential legislative, administrative, infrastructural, technological and human resources needed to effectively address cybercrimes against children and young people.

It is imperative to foster collaborative efforts and cooperation among all stakeholders to lay the foundation for safe and secure internet use.

Recommendations

This situation paper makes specific and practical recommendations for the government, policymakers, the NTA, the ICT sector, schools and colleges, media, United Nations agencies, I/NGOs, parents, guardians and children's caretakers to fulfil their responsibilities for the protection of children and young people in the digital age.

Some of the important recommendations made are as follows:

To the government and policymakers:

- Develop a comprehensive ICT law to criminalize all activities that subject children to exploitation through the misuse of ICT, with definitions such as child sexual abuse material (CSAM), child sexual exploitation material (CSEM), 'online grooming' or solicitation of children for sexual purposes, sexting, sextortion, online child sex abuse, live streaming, paedophilia, cyberstalking, cyber-bullying, hate speech, mis/disinformation, computer-generated CSAM/CSEM, etc.

- Engage with stakeholders to plan and implement internet ethics in order to achieve better results via collaboration with civil society organizations, the private sector, individuals working in the development sector, internet service providers (ISPs) and mobile operators.

- Establish a task force comprising representatives from relevant government agencies, NGOs and the private sector dedicated to address emerging challenges and develop effective solutions.

To the NTA and the ICT sector:

- Adhere to the United Nations Guiding Principles on Business and Human Rights and monitor corporations' compliance while upholding their obligations to protect children's rights by preventing any negative impacts resulting from their activities, goods, or services.

- Monitor and control pages/content with the potential to directly harm children and young people.

- Develop techniques to restrict searches by implementing a list of prohibited terms, a method increasingly employed by numerous nations. This approach prevents access to websites based on identified phrases within requested URLs. Other similar strategies are also recommended, such as IP blocking, DNS filtering and URL blocking.

8

To schools and colleges:

- Introduce online literacy and safety courses for children, parents and educators.

- Inform parents and educators about the parental control features available on their smartphones, laptops, computers and other comparable devices.

- Educate children about technical skills related to information and communication in schools and colleges and provide them with a broader understanding of cyber safety for their own protection.

- Establish counselling services within educational institutions to support children facing online safety issues, ensuring a holistic approach to their well-being.

To media:

- Conduct media literacy programmes and online safety educational campaigns for children and young people. These efforts should be accompanied by public awareness campaigns to better inform parents about the parental control tools at their disposal.[1]

- Develop and promote ethical reporting guidelines for media outlets when covering incidents related to children's online safety, ensuring responsible and non-exploitative reporting.

To NGOs and INGOs:

- Collaborate on the creation of efficient reporting mechanisms – such as hotlines that allow users to report abuse – and other online support systems to stop abusive circumstances and fight cybercrime.

- Inform relevant stakeholders of the dangers of cybercrime and teach them to spot the warning signs and symptoms of internet abuse in children and young people.

- Engage in continuous research to stay abreast of emerging threats and technological developments, and advocate for policies that prioritize the well-being of children in the digital space.

- Provide ongoing training and capacity-building programmes for law enforcement agencies to effectively investigate and address cybercrimes against children.

---

[1] Thierer, Adam D., 'Rep. Bean's 'Safer Net Act': An education-based approach to online child safety', Progress & Freedom Foundation Progress on Point Paper No. 14.3, Social Science Research Network, 28 March 2007, p. 2.

To parents/guardians:

- Educate children and young people on cyber safety so that they become more capable of making informed decisions, avoiding potential dangers and lending a hand to one another when necessary.

- Inform children about child-friendly websites and safety precautions for using the internet, like keeping online accounts private, avoiding giving out personal information to strangers online, changing passwords frequently, being cautious when downloading content from the internet, etc.

- Promote positive online conduct and be attentive and address when children disclose any issues they may have encountered on the internet.

- Establish open communication channels between parents, educators and children to facilitate ongoing discussions about online experiences, challenges and concerns.

Conclusion

The expansion and development of the internet will continue to influence lives in ever-greater ways. Nepal and other countries will both reap rewards and face challenges from the rapid global adoption of mobile phone technologies, broadband penetration and online access, as well as from the falling costs and expanding capacities of these technologies. On the positive side, the internet offers enhanced learning opportunities, creative expression and access to a wealth of information and resources that can support educational and personal growth. However, it also presents significant dangers, including exposure to inappropriate content, cyber-bullying, online predators and privacy breaches.

Studies have shown that children and young people frequently engage in risky online behaviors, such as sharing personal information and interacting with strangers. Despite the increasing incidence of cybercrimes, Nepal currently lacks the administrative, technological, legal, infrastructural and human resources necessary to effectively address these issues. This gap leaves children and young people vulnerable to various forms of online exploitation and abuse.

Collaboration and cooperation among all stakeholders – including government agencies, law enforcement, technology companies, educational institutions, civil society organizations, parents and children themselves – are essential for creating a safe and protective online environment. Public awareness campaigns can also help educate the broader community about the risks and responsibilities associated with internet use. By working together, stakeholders can create a safer digital environment that allows children and young people to enjoy the benefits of the internet while minimizing the risks. This collaborative effort will lay the foundation for safe and protective online behavior, ensuring that the internet remains a valuable and empowering resource for future generations.

METHODOLOGY

What was done.

This situation paper is primarily the outcome of a systematic review of over 160 relevant research reports and documents conducted by ChildSafeNet. The paper also includes the input and recommendations of over 20 experts and stakeholders in child online protection. Inputs from the participants of six virtual workshops have also been included in this paper.

How it was done

The content of this situation paper was collaboratively developed through close consultation between ChildSafeNet and the researcher/content writer. It involved extensive research on relevant laws, policies, reports and documents as well as interviews with experts in child protection, particularly online child protection. The experts were approached for interviews after sending them interview questions in advance. Upon receiving consent, the interviews were conducted online using platforms like Viber and WhatsApp. Subsequently, the interview notes were integrated into the situation paper by the content writer.

Furthermore, duty-bearers and stakeholders from multiple sectors along with children and young people were consulted via six virtual workshops; their resulting feedback on the topic of online child safety was incorporated into the situation paper. A final virtual workshop was held with participants from all six virtual workshops to present and validate the findings of the paper.

The final version reflects extensive revision based on the latest facts and publications, resulting in a comprehensive situation paper.

Which and what type of literature was reviewed

The main focus of the review comprised studies on online child protection, cyber safety, child protection in general, and legal analyses of the relevant themes. The review materials also included survey results on Nepalese children's internet safety issues. International and national documents were also reviewed.

Time frame

The first version of the situation paper was finalized within three months (July–September 2020), and the second version was reviewed, revised and finalized within six months (September 2023–February 2024).

Limitations

During the first phase of the project, expert interviews were conducted through phone or other online means, due to COVID-19 restrictions. Likewise, all workshops – including the final validation workshop for reviewing the situation paper – were conducted virtually; as a result, interactions were limited, and there were restrictions on both the duration of time allotted for discussion and the number of attendees.

1. INTRODUCTION

In September 2020, Nepal had 22,879,727 broadband subscribers.[2] By April 2024, this number had surged to 42,343,373, surpassing the country's population by a significant margin.[3] More than half (55.55 per cent) of the market share of active users is attributed to mobile broadband.[4] Internet penetration in Nepal is gradually increasing, rising from 35 per cent in January 2020,[5] to 38.4 per cent in 2022,[6] and then to 51.6 per cent at the start of 2023.[7] As of January 2023, Nepal is home to 12.6 million social media users.[8]

Children and young people have greater access to the internet and social media than ever before in Nepal, which raises important questions about their safety online. Previous studies have shown that unsafe internet and social media use, behaviours that violate social media user guidelines, inadequate response mechanisms, and a lack of knowledge about safe internet use among kids, parents, teachers and other stakeholders are major problems in Nepal.[9]

This situation paper, targeted at a broader audience, including the government, policymakers, the NTA, the ICT sector, schools, colleges, the media, I/NGOs and parents/guardians, has been prepared to assess the current situation, challenges and solutions for child online protection in Nepal. The freedom to access the internet and the value of the internet for children and young people are other topics covered in the situation paper. The paper also delves into the issues related to the online safety of children, exploring the interlink between internet use and social problems such as child marriage, human trafficking and gender-based violence (GBV). The provisions of current legislation and their shortcomings are also evaluated, along with the roles and obligations of duty-bearers and stakeholders in guaranteeing children's online safety. Lastly, a set of recommendations has also been provided to concerned stakeholders, including children, parents, teachers and service providers.

The objectives of this situation paper are:

• To provide information to service providers and duty-bearers about the situation of internet safety for children and young people in Nepal;

• To assess the challenges and solutions for child online protection in Nepal;

• To persuade policymakers and other duty-bearers to adopt necessary laws and policies and strengthen response mechanisms; and

• To encourage service providers to work towards making a safer cyberspace for children and young people.

[2] Nepal Telecommunications Authority, 'MIS Report: Bhadra, 2077 (17 August 2020–16 September 2020)', Kathmandu, October 2020.
[3] Nepal Telecommunications Authority, 'Telecommunication Indicators: Chaitra, 2080 (14 March–12 April 2024', Kathmandu, April 2024.
[4] Ibid.
[5] Kemp, Simon, 'Digital 2020: Nepal', Kepios, 18 February 2020, <https://datareportal.com/reports/digital-2020-nepal>, accessed 28 May 2024.
[6] Ibid.
[7] Kemp, Simon, 'Digital 2023: Nepal', Kepios, 13 February 2023, <https://datareportal.com/reports/digital-2023-nepal>, accessed 28 May 2024.
[8] Ibid.
[9] Aryal, Kapil, et al., *Internet Safety and Risks of New Technologies to Children in Nepal*, ECPAT Luxembourg, Kathmandu, December 2019.

2. RIGHT TO INTERNET ACCESS AND ITS IMPORTANCE FOR CHILDREN AND YOUNG PEOPLE IN NEPAL

The internet connects computer networks operated by the government, industries, academia and other private parties. Even though it was initially created for the purpose of interconnecting laboratories engaged in government research, over time it evolved and expanded to serve millions of users for a multitude of purposes worldwide.[10] The Digital Nepal Framework 2019, published by the Government of Nepal, indicated a rapid growth in digital adoption in the country, with mobile penetration exceeding 100 per cent, and internet penetration reaching 63 per cent.[11]

In the first quarter of 2024, 42.34 million broadband mobile connections were active in Nepal, a figure equivalent to 144.56 per cent of the total population.[12] Within that figure, 95.81 per cent of the total population are mobile broadband users, 48.60 per cent are fixed (wired) broadband users and 0.15 per cent are fixed (wireless) broadband users.

The internet is a crucial infrastructure for social interactions and contributes to creative activity, self-expression and the development of identity.[13] The internet can have a variety of benefits if used properly. For instance, it can be useful in building one's social skills, as users can learn more about their existing friends and also make new friends through online social networking.[14] Internet-based facilities like e-government, e-commerce, e-education, e-health and e-environment have made life easier and continue to contribute positively towards efficiency in the delivery of a wide range of services in both urban and rural areas of Nepal.[15]

Amid the extensive COVID-19 lockdowns, numerous schools embraced online learning as a means to sustain students' education, thereby emphasizing the internet's importance for children and young people. The lockdown measures implemented in Nepal significantly amplified the duration of time that children and young people dedicated to online activities. According to a survey conducted by ChildSafeNet and UNICEF with 1,228 respondents, 1 in 4 children and young people (24 per cent) reported using the internet for more than 10 hours a day after the lockdown began.[16] This is a significant statistical increase from before the lockdown, where only 7 per cent of children and young people reported using the internet for more than 10 hours a

---

[10] Internet World Stats, 'Internet Growth Statistics', 2 January 2024, <www.internetworldstats.com/emarketing.htm>, accessed 28 May 2024.

[11] Government of Nepal Ministry of Communication and Information Technology and Frost & Sullivan, *2019 Digital Nepal Framework: Unlocking Nepal's growth potential,* MoCIT, Kathmandu, 2019.

[12] Telecommunication Indicators: Chaitra, 2080 (14 March–12 April 2024)'.

[13] Organisation for Economic Co-operation and Development, 'The Protection of Children Online: Risks faced by children online and policies to protect them', *OECD Digital Economy Papers*, No. 179, OECD Publishing, Paris, 2 May 2011.

[14] Duncan, Susan Hanley, 'MySpace Is Also Their Space: Ideas for keeping children safe from sexual predators on social networking sites', *Kentucky Law Journal*, vol. 96, no. 4, art. 3, 2008.

[15] International Telecommunication Union – Development Sector, *Understanding Cybercrime: Phenomena, challenges and legal response*, ITU, Geneva, September 2012.

[16] ChildSafeNet and United Nations Children's Fund, *The Impacts of COVID-19 on Protection of Children and Young People Online: A survey report*, unpublished manuscript.

day.[17] Additionally, 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.[18]

2.1. Right to internet access

The internet offers access to resources for learning, including knowledge, perspectives, educational tools and even direct contact with teachers. The internet is advantageous because it enables users to communicate, exchange knowledge and experiences, and interact with friends and peers. It can also promote innovation, creation and the exchange of ideas.[19] The internet serves as a mode of cultural exchange and a source of entertainment for users, and also strengthens their ability to assert their rights, express opinions and connect and communicate with others.[20]

The right to freedom of expression and communication for children is mentioned in article 13 of the Convention on the Rights of the Child; this right is incorporated under article 17(a) of the Constitution of Nepal (2015). Access to the internet should thus not be considered a mere privilege as it serves as a prerequisite for the enjoyment of other basic rights. The measures in the Digital Nepal Framework 2019, which aims to make internet access a fundamental right for all citizens of Nepal and improve the required IT education in schools and universities, further bolster this position.[21]

Under its current conception, human rights such as the right to information, the right to education and the right to free speech are all directly related to the internet. During the COVID-19 lockdown, for example, Nepal had a significant digital gap as the majority of private- and urban-sector schools maintained their educational programmes online while government schools lacked the necessary means to do the same. The government should be aware that the internet upholds equality, allows for expression, and needs to provide a secure and fair environment for everyone, including children.

"*A gap is built up between haves and haves not. Looking at the larger context, children face a digital divide and inequality in access to technology, which affects children's self-esteem.*" – **A female high school student**

2.2. Importance of the internet for children and young people in Nepal

The internet can empower children and young people to better exercise various rights, including the right to education, health care, access to health information, participation, association, freedom of speech, and rest and recreation.[22]

---

[17] Ibid.

[18] Ibid.

[19] Internet Society, 'Children and the Internet'*,* Internet Society, Geneva, 17 October 2021, p. 1.

[20] United Nations Children's Fund, *Children's Rights and the Internet: From guidelines to practice – Articles from the Guardian Sustainable Business Child Rights Hub*, UNICEF and *The Guardian*, New York, May 2016, p.6.

[21] *2019 Digital Nepal Framework.*

[22] Children's Rights Alliance for England, 'Children's Right and Their Online and Digital Interactions: Briefing ahead of Baroness Kidron's debate', CRAE, London, 2014, p.1.

"Internet is a must for people to exercise their basic human rights of freedom of opinion and expression." – **Key informant interview (KII) participant, Ministry of Communication and Information Technology**

For children and young people, the internet can be helpful for tasks and activities such as completing school assignments, conducting cost-effective research on diverse subjects, accessing information from around the world, pursuing online educational courses and vocational training, developing innovative ideas and skills, and much more.

If used with appropriate protections in place, ICT can be potentially pivotal for children and young people. Some research even suggests that the internet can contribute to breaking cycles of poverty and disadvantage.[23]

Even though the internet is a reliable tool for education, intellectual growth and capacity building, most Nepalese parents are unsure of its purposes or advantages.

"Most parents in Nepal have the concept that children will go down the wrong path if they use the internet, as it is perceived to be only for entertainment purposes." – **KII participant, researcher**

The use of audio, video and text-based information from the internet for interactive learning is possible. Children and young people who have access to the internet can easily retrieve information and stay up to date on both domestic and foreign affairs. Students in Nepal get the opportunity to learn about a variety of topics and events that they would seldom study in class, such as racism, the LGBTQIA+ movement, the Black Lives Matter movement, the Yemeni Civil War, and much more. Through the knowledge they gain via the internet, children are continuously expanding their worldviews. The internet is also seen to play a significant part in socialization and fostering connections among individuals, as well as serving as a platform for finding entertainment, job prospects and company marketing techniques.

"First, we need to know what the needs of the beneficiaries (children) are, and how we could make the internet more exciting for them so that the positive aspects of learning can be promoted." – **KII participant, development sector worker**

---

[23] Third, Amanda, et al., *Young and Online: Children's perspectives on life in the digital age – The State of the World's Children 2017 companion report*, Western Sydney University, Sydney, December 2017.

3. ONLINE SAFETY: GENERAL CONCEPTS AND CONCERNS

3.1. Underlying concept of cyber risks and online safety

With the pervasive use of internet technologies and various social networking sites, cases of cybercrimes have been on the rise[24] and have raised serious concerns over issues related to social media privacy, security and accessibility. To maximize the benefits of connectivity, it is important for users to understand the risks of using the internet.[25]

Online privacy, cyber-bullying, sexting, sextortion, online sexual predation and grooming, personal information security, accessing age-appropriate content, internet and device addiction, online gaming safety, security tools and filtering software, digital fraud, hacking and online piracy are just a few of the many issues that fall under the category of cyber risks.[26]

Understanding the concept of online safety is crucial because it calls for safe online behaviour to avoid phishing scams or other illegal actions.[27]

Children's and young people's lives have become thoroughly engulfed by the increasing usage of mobile phones and the internet. Spending more time online exposes children and young people to risks such as exposure to sexual content, sextortion, revenge CSAM/CSEM, online grooming, livestreaming of sexual abuse and exploitation, cyber-bullying, harassment, identity theft and phishing.[28] Due to the ease with which cybercriminals can access and manipulate personally identifiable information about social media users that is publicly available – such as age, gender, address and phone number – online social networks have emerged as their preferred operating environment.[29] There has been an increase in the reporting of cybercrimes in Nepal.

3.2. Growing need for online safety

As of 7 February 2024, the Cyber Bureau of Nepal Police has registered 13,330 cybercrime cases since July 2023. Among these, 11,425 are related to social media, and 1,905 are related to online financial activities. Out of these, 125 complaints were from boys and 197 complaints were from girls. The mediums for the commission of these cybercrimes were Facebook and Messenger (9,350), TikTok (667), WhatsApp (491), Instagram (432) and many more.

As per the fact sheet on cybercrime and suicide published by the Women, Children, and Senior Citizen Service Directorate at Nepal Police Headquarters, 7,382 cases were registered with the

---

[24] Setopati, 'Youths More Vulnerable to Cyber Crimes', Lalitpur, 3 February 2019, <https://en.setopati.com/social/138783>, accessed 28 May 2024.

[25] Telstra Group Limited, *Addressing the Cyber Safety Challenge: From risk to resilience*, Melbourne, July 2014, p. 12.

[26] Ibid., p. 6.

[27] Merriam-Webster, 'Cybersafety', *Merriam-Webster.com Dictionary*, <www.merriam-webster.com/dictionary/cybersafety>, accessed 28 May 2024.

[28] Smith, Peter K., Fran Thompson and Julia Davidson, 'Cyber Safety for Adolescent Girls: Bullying, harassment, sexting, pornography, and solicitation', *Current Opinion in Obstetrics and Gynecology*, vol. 26, no. 5, October 2014, pp. 360–365.

[29] Al Mutawa, Noora, Ibrahim Baggili and Andrew Marrington, 'Forensic Analysis of Social Networking Applications on Mobile Devices', *Digital Investigation,* vol. 9, supplement, August 2012, pp. S24–S33.

Cyber Bureau in Kathmandu alone between mid-July 2022 and mid-July 2023. Other provinces with a high number of cybercrime registrations were Koshi Province with 402 cases and Lumbini Province with 382 cases. The fewest cases of cybercrime were registered in Sudurpaschim Province, with only 110 cases.[30]

The dire need for greater online safety in Nepal is further illustrated through the results of a survey conducted by ECPAT Luxembourg.[31] Of the 5,011 children who took the survey, 72 per cent reported using mobile phones and internet technologies, and 49 per cent reported using the internet without knowing that harming, abusing or insulting someone online may amount to a crime. A similar trend was identified in the findings from ECPAT Luxembourg's Knowledge, Attitude, and Practice (KAP) survey, conducted with 452 children (212 girls and 240 boys) in Kathmandu Valley.[32] Among those children surveyed, 15 per cent said they had experienced online abuse. In terms of gender, 47 per cent of those who reported online abuse were boys and 53 per cent were girls. According to the KAP study, 3 per cent of respondents said they frequently share images with strangers online, while almost 40 per cent said they occasionally exchange pictures with online strangers.[33]

Another study conducted by ChildSafeNet in 2019 found that 41.15 per cent of the children and young people surveyed had viewed online sexual content.[34] These results were consistent with another ChildSafeNet and UNICEF survey conducted in 2020, which found that 41.7 per cent of children and young people reported viewing online sexual content.[35]

The growth of user-generated content and content-sharing platforms, the adoption of smartphone technologies, cloud storage, platform integration and single sign-on mechanisms, as well as the emergence of the Global Positioning System (GPS) and location-based services, have all had a significant impact on how users interact online.[36] Cyber safety plans need to be carefully considered because of the ever-changing landscape of technological trends, products and practices.

"*Children and young people are not completely safe online. With the increasing use and exposure to new contents and online platforms, the threats and dangers also increase simultaneously.*" – **KII participant**

Fraud/spam, cyber-bullying, cyberstalking, grooming, sexting, spreading fake news, internet addiction, gaming addiction, hacking, sextortion (i.e., online sexual exploitation), online hate speech (e.g., making critical comments on social media posts), sexual harassment in private or public messages, and CSAM are some of the online risks for children and young people identified by the KII respondents. Studies show that internet technologies and digital devices have become

---

[30] Women, Children and Senior Citizen Service Directorate, 'PHQ Fact Sheet on Cybercrime and Suicide', Government of Nepal Ministry of Women, Children and Senior Citizens, Kathmandu, July 2023.

[31] Aryal et al., *Internet Safety and Risks of New Technologies.*

[32] Aryal, Kapil, *Assessing and Understanding the Risk: Sexual exploitation of children online in Nepal*, Voice of Children and ECPAT Luxembourg, Kathmandu, 2017.

[33] Ibid.

[34] ChildSafeNet, *Living in the Digital Age*, ChildSafeNet, Lalitpur, 2019.

[35] *The Impacts of COVID-19 on Protection of Children and Young People Online.*

[36] *Addressing the Cyber Safety Challenge*, p. 4.

accessible to people before they possess knowledge of safe internet practices and the potential online harms that may be caused by their misuse.

The fact that children and young people are not entirely safe online is a prevalent concern among Nepalese stakeholders. With rapid technological advancements, exposure to new online information and platforms has simultaneously increased threats and dangers.

"*Gender issues can be seen reflected on the internet. Women and girls get spam messages, are harassed, receive aggressive texts from strangers, and on the whole experience online abuse and exploitation in many different ways. This is prevalent among people in my age group. For example, many girls around my age are asked to send explicit pictures.*" – **A male student, age 17**

Although the internet offers numerous benefits, it also presents several potential drawbacks that can affect children and young people. These include information overload, negative impacts on mental health and physical discomfort such as eye strain and body aches from prolonged exposure to sensitive or distressing content online. In addition, internet usage can influence dopamine levels and radiation exposure, and unrestricted access to pornography can lead youngsters to develop misconceptions about sex, sexuality and sexual health.[37]

"With increasing exposure to the internet, the risks also increase." – **KII participant, cybersecurity expert**

---

[37] Jović, Jelena, and Nataša Đinđić, 'Influence of Dopaminergic System on Internet Addiction'**,** *Acta Medica Medianae*, vol. 50, no. 1, March 2011, pp. 60–66.

4. ENHANCING ONLINE SAFETY: ADDRESSING HARMS, CYBERCRIMES AND SOCIETAL IMPLICATIONS FOR CHILDREN AND YOUNG PEOPLE IN NEPAL

4.1. Vulnerability of children and young people in Nepal

Despite the numerous advantages access to the internet provides, people also need to be aware of the accompanying spectrum of risks. To assess the vulnerability of children and young people in Nepal to these risks, some facts and data need to be considered.

Nepal ranked 94th in the 2020 Global Cybersecurity Index with a score of just 44.99.[38] The Index measures a country's commitment to cybersecurity and is intended to raise awareness of cybersecurity issues.

In 2023, ChildSafeNet conducted research on online intimate partner violence (IPV) against teens and young people in Nepal (4,352 participants, aged 16 to 24 years in 10 districts of Nepal, were involved). The results found that 24 per cent of teens and young people experienced online IPV and 41 per cent experienced offline IPV, resulting in anger, depression, social distancing and self-harm. Furthermore, it was revealed that 27 per cent of males faced online IPV compared to 21 per cent of females, indicating that in a society where females are traditionally viewed as primary victims, males also experience intimate partner violence.

The common forms of online IPV included stalking, monitoring, and controlling the partner's accounts. Many did not report the online violence they experienced, due to shaming, victim blaming, safety concerns, low awareness of the reporting mechanisms and distrust in the justice system.

Similarly, according to a study conducted by Child Workers in Nepal (CWIN) in 2020, boys face comparatively more pressure to post and share self-generated sexualized materials (i.e., nude images, audio and videos), with Kathmandu, Dhanusa and Morang districts having the highest prevalence at 24.53 per cent, 19.8 per cent and 12.26 per cent, respectively.[39]

A nationwide study conducted by ECPAT Luxembourg in 2019 showed that children have the desire to increase their number of friends on social media, which can result in sending and accepting friend requests to and from strangers.[40] At the same time, a report by ECPAT International claimed that children in Nepal are at a significant risk of sexual exploitation. In the 2019 Out of the Shadows Index, which measures the prevention of and response to child sexual exploitation and abuse, Nepal received a score of 46.4 and was ranked 39th out of 60 nations.

---

[38] International Telecommunication Union – Development Sector, *Global Cybersecurity Index: 2020,* ITU, Geneva, 2021.
[39] Child Workers in Nepal and Good Shepherd International Foundation Nepal, *A Study on Online Child Sexual Exploitation in Nepal*, CWIN Nepal, Kathmandu, 2020.
[40] Aryal et al., *Internet Safety and Risks of New Technologies.*

The country's lax regulations against internet exploitation have been cited as one of Nepal's most urgent risks.[41]

As previously noted, the KAP survey conducted by ECPAT Luxembourg and Voice of Children in Kathmandu Valley found that 15 per cent of the child respondents had experienced online abuse, of which 47 per cent were boys and 53 per cent were girls.[42] According to another 2017 survey conducted in the Kathmandu Valley, 20 per cent of children with internet access watch pornographic content at least once. This study also found that 57 per cent of victims of online sexual assault were female, and that the problem affects 13.7 per cent of school-age children who use the internet.[43]

Social-networking-site-related risky behaviours include unsafe information disclosure, internet addiction, risky sexual behaviour, cyber-bullying, exposure to harmful online communities, and cyber threats. Children are at a higher risk of facing online interpersonal victimization if they engage in risky behaviours like sharing personal information through email or posts, making disrespectful or offensive remarks, connecting with strangers they've met online, and discussing dating and sex with strangers.[44]

A study carried out with 5,011 children in Nepal by ECPAT Luxembourg found that 7.42 per cent of respondents had received requests from online strangers to meet in person or had received promises of gifts while chatting online. Furthermore, 22.1 per cent admitted to engaging in conversations with online strangers without informing their family members.[45] These inappropriate online behaviours heighten the vulnerability of children and young people to online risks and, at times, result in self-harm. For instance, data shows that children and young people are the largest population demographic found to be involved in cybercrimes, particularly ages 15–25.[46]

It is important to keep in mind that all attempts to ensure cyber safety should strike a balance between watching over children's and youths' online behaviour and letting them use ICTs on their own and in an age-appropriate manner.[47]

"*The groups mostly targeted are girls [as compared to boys], women, non-binary individuals and children who have diverse gender identities and sexual orientations.*" – **KII participant**

"*Males tend to overlook the fact that they can fall victim to online risks such as grooming or abuse. They do not believe that they can also be at risk.*" – **KII participant**

---

[41] Himalayan News Service, 'Children at High Risk of Sexual Exploitation in Nepal: Report', *The Himalayan Times*, Kathmandu, 2 February 2020, <https://thehimalayantimes.com/nepal/children-at-high-risk-of-sexual-exploitation-in-nepal-report/>, accessed 28 May 2024.

[42] Aryal, *Assessing and Understanding the Risk.*

[43] Himalayan News Service, 'School Children at High Risk of Online Sexual Abuse', *The Himalayan Times*, Kathmandu, 11 February 2018, <https://thehimalayantimes.com/nepal/schoolchildren-high-risk-online-sexual-abuse/>, accessed 28 May 2024.

[44] Ybarra, Michele L., et al., 'Internet Prevention Messages: Targeting the right online behaviors', *Archives of Pediatrics and Adolescent Medicine*, vol. 161, no. 2, pp. 138–145.

[45] Aryal et al., *Internet Safety and Risks of New Technologies.*

[46] 'Youths More Vulnerable to Cyber Crimes'.

[47] Robinson, Elly, and Vicky Nagy, 'Enhancing Online Safety for Children: Response to the public consultation on key election commitments', Australian Department of Social Services – Australian Institute of Family Studies, Melbourne, March 2014, p. 3.

4.2. Online safety issues for children and young people, including self-harm

The websites and content that children and young people actively access, either directly or indirectly through another person, determine their level of online safety. According to a 2019 study by ECPAT Luxembourg, the majority of children (56.6 per cent) were unaware of the regulations governing their online safety or the channels for victims of online sexual abuse and exploitation to pursue justice.[48] Many parents lack the sensitivity necessary to address these circumstances and are unaware of the risk their children are exposed to online. A sizeable percentage of parents (32.5 per cent) were found to have disregarded any unfavourable online incidents that their children had told them about and to have done nothing to address these complaints.[49]

Cases of online exploitation, identity theft, cyber-bullying and harassment are mostly being dealt with or investigated by the Cyber Bureau and the Metropolitan Police Range in Kathmandu. Despite the creation of provincial police offices and district police offices mandated to investigate cybercrimes, they do not have the human, capital or technological resources to do so. Additionally, schools and teachers have low levels of awareness of online safety; hence, there is a severe lack of advocacy for including online safety in school curricula.[50]

The unprecedented rise in popularity of social networking sites has brought both opportunities and threats, so it is critical that all stakeholders – parents, teachers, civil society, media and the government – work together to create environments that are accessible and safe for children, wherever they are. Safeguarding the internet is a collective responsibility to ensure that children can benefit from it in a healthy manner, free from harm.

An important way of preventing children from causing self-harm is by making them understand the concepts of risk and safety online. This is useful in empowering children to make moral choices on their own. Stakeholders and duty-bearers should make an effort to introduce children to the internet at a gradual pace and teach them resilience skills to deal with the risks of the online world. For this aim, the main objective should be educating children about the value of 'netiquette' (internet etiquette) and instilling in them the idea of 'think before you click.'[51]

Parents can help their children navigate the guidelines for internet usage while using technical safety tools such as parental control software.[52] It is, however, crucial to acknowledge that extreme parental monitoring may sometimes backfire and have a negative effect on the development of a child's understanding of how to use technology safely; the more restricted children are from internet access, the more curious they may become about certain 'prohibited' content and activities.

"Findings from the research that I conducted on online sexual exploitation of children in Kathmandu stated that among small children, there is a trend of sharing content on the internet without knowing how it can be misused. Adolescents visit sites with abusive content and share videos, images and web links with their friend circles. Since there is no monitoring from parents, and there is a desire for privacy, adolescents engage in making fake IDs on social media platforms

[48] Aryal, et al., *Internet Safety and Risks of New Technologies.*

[49] Ibid.

[50] Ibid.

[51] 'Children and the Internet', p. 3.

[52] 'The Protection of Children Online'.

and post unethical content, harassing others by frequently messaging them, sending threatening emails, blackmailing, etc." - **KII participant, lawyer/researcher**

4.3. Linkage of internet use with commercial sexual exploitation and child marriage

The increased proliferation and use of internet technologies have led to a rise in the exploitation of children and young people in the commercial sex trade. Traffickers, for instance, leverage the internet, text messaging, and digital and web cameras to arrange 'dates' for their 'girls.' Additionally, the internet has been significantly misused as a means to distribute CSAM.[53]

Online recruiting and advertising have evolved, and new forms of exploitation – like real-time live broadcasting of sexual exploitation – have emerged. Offenders have a lot of options linked to the internet to find and groom marginalized people since they can search media for young and vulnerable people. Additionally, technology makes it easier to access illegal activities across national borders, and cybersex dens are frequently hard to track because they stream illegal content rather than download it. As a result, users leave a small digital footprint when accessing such content and can avoid the digital traps set up by law enforcement to catch people watching child pornography.[54] Children are more actively participating online and connecting with adult strangers, which increases their vulnerability to human trafficking. Similarly, increased access to internet-enabled mobile phones has been cited as one of the primary causes of an increase in teen romances and subsequent child marriages in Nepal.[55]

Nepal has the third-highest prevalence of child marriage in the world, with 41 per cent of women aged 20 to 24 married before they turn 18. Nepal also ranks in the top 10 countries for the prevalence of child marriage among boys.[56] Nepal is home to 5 million child brides. Of these, 1.3 million married before the age of 15.[57] These days, many self-initiated marriages between adolescent people begin through social media platforms.[58] Social media has been identified as the main enabler of child marriages in Nepal. Reports from Human Rights Watch Nepal, Save the Children in Nepal and *The New York Times* indicate a rising trend of children getting married to individuals they meet on social media platforms, particularly Facebook.[59]

4.4. Linkage of internet use with trafficking in persons

[53] International Labour Organization, *Commercial Sexual Exploitation and Trafficking of Children 'In a Nutshell': A resource for Pacific Island countries*, ILO, Geneva, 2015, pp. 30–31.

[54] Allen, Caitlin, 'The Role of the Internet on Sex Trafficking', International Observatory of Human Rights, London, 7 March 2019, <https://iohr.rightsobservatory.org/blog/the-role-of-the-internet-on-sex-trafficking/>, accessed 28 May 2024.

[55] Oli, Krishna, 'Child Marriages Increasing in Bajura, Mobiles, Internet Blamed', *República*, Kathmandu, 4 October 2016, <https://myrepublica.nagariknetwork.com/news/child-marriages-increasing-in-bajura-blame-on-phones-internet/>, accessed 28 May 2024.

[56] United Nations Population Fund and Quilt.AI, 'Policy Brief: Nepal – Digital ecosystem analysis on child marriage in Nepal', UNFPA Asia and the Pacific, Bangkok, April 2023.

[57] United Nations Population Fund and United Nations Children's Fund, 'Nepal Country Profile: UNFPA-UNICEF Global Programme to End Child Marriage', UNFPA and UNICEF, New York, 2020.

[58] Ibid.

[59] Aryal, Nabin, 'Instagroom: Is social media fueling child marriage in Nepal?', Rukmini Foundation, Pittsburgh, 28 February 2021, <www.rukminifoundation.org/2021/02/28/instagroom-is-social-media-fueling-child-marriage-in-nepal/#:~:text=Reports%20from%20Save%20the%20Children%20Nepal%2C%20Human%20Rights,they%20met%20on%20social%20media%20platforms%2C%20mainly%20Facebook.>, accessed 28 May 2024.

The linkage between internet use and trafficking in persons is a complex and multifaceted issue that involves the exploitation of individuals through digital platforms. The internet has both facilitated and complicated human trafficking in various ways. Traffickers often use the internet to recruit victims and advertise their services or false job opportunities. They can use social media sites like Facebook, Instagram, Snapchat, job portals and other online platforms to lure individuals into trafficking situations by promising employment, education or a better life.

Traffickers may employ strategies like proclaiming their affection and admiration for the victims and promising to turn them into celebrities. With the intention of exploitation, the traffickers may occasionally even use amazing work opportunities to entice victims. Several techniques, such as threats, physical punishment and emotional blackmail, are used to prevent victims from contacting family members or making requests after they are under the offender's control or confidence.[60] The internet enables traffickers to receive payments and manage financial transactions related to trafficking. Digital currencies and online payment platforms provide anonymity, making it easier for traffickers to transfer funds and evade detection.

4.5. Linkage of internet use with labour exploitation

Considering how frequently job offers are advertised online, there is a logical connection between the internet and emerging trends of labour exploitation. It is relatively simple and inexpensive to utilize the internet to post false job offers and build false websites to trick people looking for employment prospects. The greater audience of the internet is likely to draw both those who are actively seeking employment as well as those who may be looking for a new challenge. Offenders can lure potential victims with work offers and then traffic them into circumstances of labour exploitation while keeping a high level of anonymity.[61]

4.6. Linkage of internet use with gender-based violence

The growth in technology-facilitated GBV has been influenced by the increased usage of ICTs. The misuse of digital technology – which can include a variety of activities such as taking, uploading or disseminating photos and videos without permission, editing and uploading photos and videos, harassing, stalking, extorting, accessing or disseminating private data, creating false profiles or engaging in other types of identity theft, spreading hate speech, producing pornography, and much more – has disproportionately affected women.[62] The fact that ICTs allow for the quick spread of content and the option of anonymity for the offender, making it harder to track perpetrators, further advances these technology-related acts of violence. Abusers can use digital means to control and manipulate their partners in abusive relationships. This includes monitoring their online activities, tracking their locations through devices, and using technology to exert coercive control. Furthermore, misogynistic attitudes and hate speech against women and gender-diverse individuals are perpetuated on various online platforms. This can contribute to a hostile online environment that can have real-life implications for victims.

---

[60] Dixon, Herbert B., Jr., 'Human Trafficking and the Internet* (*and Other Technologies, Too)', *The Judges' Journal*, vol. 52, no. 1, January 2013.
[61] International Trade Union Confederation, Anti-Slavery International and Churches' Commission for Migrants in Europe, *The Role of the Internet in Trafficking for Labour Exploitation*, ITUC, Brussels, 2014.
[62] Women's Legal and Human Rights Bureau, Inc., 'From Impunity to Justice: Domestic legal remedies for cases of technology-related violence against women', Association for Progressive Communications, 2015.

5. A REVIEW OF EXISTING LAWS ON THE PROTECTION OF CHILDREN AND YOUNG PEOPLE FROM CYBERCRIME

Legal frameworks and policies must be adaptable and flexible enough to address the new opportunities and risks posed by evolving technologies, which have permeated every aspect of modern life. This section outlines the strengths of existing legal regimes that protect children and young people in Nepal and highlights the gaps in protecting them from online abuse and exploitation.

Constitution of Nepal, 2015: The Constitution of Nepal guarantees the right to a dignified life (article 16), the right to freedom of opinion and expression (article 17(a)), the right to communication (article 19), and the right against exploitation (article 29), among many other fundamental rights. These are foundational provisions that extend to the protection of children and young people in cyberspace as well. Moreover, article 39 has specifically made provisions related to the rights of the child, which extend over 10 sub-articles. Article 39(6) holds that no child shall be subjected to abuse, exclusion, or physical, mental, sexual or other form of exploitation or improper use by any means or in any manner. Article 39(7) states that no child shall be subjected to any form of torture at any place and situation. These rights are equally relevant in protecting children and young people from online offences or crimes committed through the internet.

The above-mentioned rights have been guaranteed as the fundamental rights of the child under the Constitution of Nepal, which implies that the state has a responsibility to make legislation necessary for their implementation[63] and, more importantly, that the enforcement of these rights is a matter of constitutional remedy,[64] making them very significant.

Act Relating to Children, 2018: The Act defines the term 'child sexual abuse material', including aspects of possible online abuse.[65] Similarly, section 66(3) outlines the various types of sexual abuse that are committed against children and guarantees children's right to protection, including from sexual exploitation (section 7). In accordance with the provisions of the Act, private or social organizations, schools, or public institutions are required to adopt child protection standards to ensure the protection of children at the institutional level. Section 57 of the Act also calls for the creation of a complaint registration system to keep track of complaints made regarding child protection. Despite being a new act, the definitions of 'corruption of children', 'grooming' or 'solicitation of children for sexual purposes', 'sexting', 'sextortion', 'online child sex abuse or livestreaming', 'sex tourism', 'paedophilia' and 'cyberstalking/bullying' have not been

---

[63] Nepal, *Constitution of Nepal*, Article 47 (2015). This says that the State shall, as required, make legal provisions for the implementation of the rights conferred by this Part, within three years of the commencement of this Constitution.
[64] Nepal, *Constitution of Nepal,* Article 46 (2015).
[65] Section 2(m) of this Act has defined 'child pornography' as "taking of photo or video of sexual organs of children or taking of video or photo of children by making them indulge in sexual activity in virtual world, publication of sexual activity in poster, pamphlets, magazines or dissemination of obscenity through films or by other means of media and the term also denotes production, sale, import-export, collection or dissemination of such materials".

incorporated, and punishment has not been prescribed as per the nature and gravity of the crime mentioned here.

The Act has scope for prosecuting cybercrimes against children in all districts of Nepal, but investigators and prosecutors typically use the Electronic Transaction Act (ETA), simply because the ETA prescribes a longer imprisonment term of five years compared to the one-year term prescribed by the Act Relating to Children 2018. Offences committed against children and by children should be prosecuted using the Act Relating to Children 2018, which has a longer statute of limitations for filing cases. That statute of limitations with respect to an offence against a child is one year after the child has attained the age of 18.[66]

Electronic Transaction Act (ETA), 2008: The ETA makes a number of cybercrimes illegal, including computer fraud; accessing unauthorized computer materials; damaging computers and information systems; publishing illegal materials electronically; disclosing confidential information; and pirating, destroying or altering computer source code. The publication of illicit content in electronic form is prohibited by section 47 of the ETA, and anyone found guilty of violating this provision faces a fine of up to NPR 100,000, up to five years in prison, or both.[67] Having been enacted almost 16 years ago, the ETA does not reflect the current technological developments and challenges, such as online payment, data protection, privacy, and cybercrimes including sexual exploitation of children online. Currently, all types of online abuses against women and children are prosecuted under section 47 of the ETA, which is very limited and inadequate. In the absence of a comprehensive Act against cybercrime, victims as well as offenders have been negatively affected by the insufficient and improper application of the law.

There still seems to be some confusion and contradiction in whether to use the ETA or the Act Relating to Children 2018 when crimes are committed against children through electronic means, as both acts provide jurisdiction over such crimes. The ETA is not primarily focused on the protection of children online, but it is a special act that deals with electronic-transaction-related crimes.

On 26 June 2023, the government of Nepal provided powers to all district police offices to investigate, all offices of district government attorneys to prosecute, and all district courts to hear cases under the ETA. Previous to that, all cases under the ETA were investigated by the Cyber Bureau, prosecuted by the Kathmandu District Attorney's Office, and adjudicated by Kathmandu District Court.

National Criminal Procedure (Code) Act, 2017: The Code outlines the fundamental rules of criminal procedure that apply to all forms of criminal activity, including cybercrime. There are, however, no special rules for safeguarding children and adolescents against cybercrime. Prostitution, pornography and nudity are all prohibited under sections 215 and 119, respectively, and it is also forbidden to advertise prostitution or to persuade someone else to do so. The Code's

---

[66] Nepal, Act Relating to Children, Section 74 (2018).
[67] Section 47(1) prohibits any person from publishing or displaying "any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to public morality or decent behaviour or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities", or which may engage in teasing women, disrespecting them or doing any indecent activities.

section 225 forbids the sexual exploitation of children. A person is considered to have sexually exploited a child if they bring the child to an unusually remote location, force them to touch or grab (hold) his/her genital organ, or engage in any other odd sexual behaviour.

If there is a special Act to deal with the offence, general law is not applied, and the Criminal Code 2017 is a general law of Nepal. Thus, in the case of a crime committed against a child, the Act Relating to Children 2018 – being a special Act to deal with crimes committed against children – is utilized. If the crime against children is committed by misusing digital devices and internet technologies, the ETA is used as a special Act to deal with cybercrime.

Draft Information Communication Technology (ICT) Bill, 2018: The Bill, if passed, would contribute to cybersecurity and the control of cybercriminals, upholding the public interest. The following provisions under this Bill are particularly relevant to issues related to the protection of children against cybercrime:

Section 83	Prohibits cyber-bullying by stating that no one should use electronic systems to tease, humiliate, discourage, insult or harass another person.
	A person committing such an offence is liable for a fine of up to NPR 1,000,000, five years of imprisonment, or both (section 96(23)).
Section 84	Forbids cyberterrorism – i.e., no action should be taken through electronic systems so as to disrupt the country's security, sovereignty, geographical integrity or statistical systems.
Section 85	Forbids the use of electronic mediums for sexual abuse and holds that no one shall be subjected to arbitrary interference with his/her privacy through electronic mediums. A person committing such an offence is liable for a fine of up to NPR 30,000, three years of imprisonment, or both.
	If the offence is committed against children, the perpetrator shall be punished with an additional 25 per cent (section 96(25)).
Section 86	Forbids generating, compiling, transmitting, displaying, distributing, publishing, disseminating, buying or selling any pornographic material through electronic systems.
	A person committing such an offence is liable for a fine of up to NPR 1,000,000, three years of imprisonment, or both (section 96(26)).
Section 87	Prohibits the use of electronic mediums for enticing, making proposals, requesting to meet or establishing online relations with the intention of sexual exploitation, fraud or any such illegal activity.
	A person committing such an offence is liable for a fine of up to NPR 1,000,000, three years of imprisonment, or both (section 96(27)).

The Bill has been pending as a draft for five years. If it ultimately becomes an act, its final provisions are uncertain.

Draft IT and Cybersecurity Bill, 2024: If adopted, this Bill will play a significant role in the criminalization of unauthorized access to and use of electronic systems for the purpose of wilfully committing unlawful crimes with malicious intent. In addition, the production, sale, procurement for use, import, export, distribution and use of illegal devices for the purpose of committing an offence under this Bill, as well as electronic forgery and electronic fraud committed as an identity-related crime, are all prohibited. The Bill also criminalizes child pornography and the solicitation of children.

Reviewing the above-mentioned legislations, it is clear that Nepalese laws do not define critical concepts/terminologies like 'child abuse material', 'corruption of children', 'grooming' or 'solicitation of children for sexual purposes', 'sexting', 'sextortion', 'online child sexual abuse or livestreaming', 'sex tourism', 'paedophilia' and 'cyberstalking/bullying'. The definition of CSAM provided by the Act Relating to Children 2018 (section 2(m)) does not meet the standard set by the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, as it only includes visual materials. There are also no sufficient laws to monitor and regulate ISPs. Nepal does not impose any legal requirements on ISPs to report CSAM. These loopholes explain why Nepal received a score of 0/100 in the Out of the Shadows Index's indicator for online grooming,[68] and 33/100 for internet protection.[69]

Nevertheless, a wide range of cybercrime-related topics are covered, and subsequent offences have been penalized by the Draft ICT Bill 2018 and the Draft IT and Cybersecurity Bill 2024. Therefore, endorsing these bills can significantly aid in improving Nepal's cybersecurity.

Cyber Security Bylaw, 2020: To protect the ICT infrastructures and information systems of Nepal's telecommunication service providers from various malicious attacks and threats, and to foster user confidence in using ICT technologies and services, the NTA drafted this Bylaw for the implementation of cybersecurity standards and best practices. As a result of this Bylaw, licensees are now responsible for implementing security awareness programmes for their staff and pertinent parties. The Bylaw also states that the licensee must take the appropriate steps to educate consumers about dangers, help them understand the attendant risks, and assist them in securing their networks. These activities may include:

(i)   Raising awareness through websites/portals for practising safe online behaviours.
(ii) Collaboration with other entities/organizations for awareness and education.
(iii) Conducting workshops/seminars/trainings/interaction programmes to educate customers/users on ICT-security-related matters, e.g., the importance of using licensed software, updating and patching operating systems and applications, etc.
(iv) Adopting any other methods as appropriate and necessary.

In addition to legislation, the Government of Nepal has enacted various policy measures to handle cybersecurity risks and ensure online safety for children and young people.

National Cyber Security Policy, 2023: The policy is focused on formulating legislation and standards for the purpose of creating a secure and resilient cyberspace. The policy also aims to

---

[68] The Out of the Shadows Index is a 60-country benchmarking index that measures how nations are addressing child sexual exploitation and abuse. It is developed by Economist Impact.
[69] ECPAT Nepal, 'Sexual Exploitation of Children in Nepal', ECPAT International, Bangkok, 2020.

establish institutions and structures for the protection of information and communication technology. The policy also includes the production of qualified human resources in the ICT sector for deployment in research; raising public awareness through a digital literacy programme for cybersecurity; coordination and collaboration with public and private institutions and civil society organizations for creating secured cyberspace; coordination and collaboration with other countries and international organizations for strengthening cybersecurity; continuous monitoring to create secured cyberspace; and making accountable the software developers and suppliers, hardware producers and suppliers, and service providers as necessary. The Policy outlines the inclusion of cybersecurity in school and higher education curricula.

Online Child Safety Directives, 2019: The Directives mainly aim to provide for the safe use of internet for children, imposing duties and responsibilities on guardians, schools, NGOs and ISPs to protect children from the potential risks of online platforms. For instance, it mentions the duty of the ISPs to provide the necessary information and technological support to children and their guardians to protect children from the potential risks of the internet[70] and to formulate and implement procedures for addressing complaints regarding child abuse content.[71] Similarly, the Directives also state that it will be the responsibility of NGOs to develop necessary awareness and security systems, in collaboration with various stakeholders, to protect children from the potential risks of online platforms.[72]

Directives on the Operation of Social Networking, 2023: The Government of Nepal passed this Directive in November 2023 to address the management of the operation of social media. The Directive prescribes that social media platforms wanting to operate in Nepal should register in Nepal. Additionally, it mandates that there be either an office or a point of contact on the social media platform to address complaints received. The Directive also prescribes dos and don'ts for social media users and further delineates the responsibilities of the social media platform operators.

ICT Policy, 2015: This Policy realizes the faster uptake of ICTs in the country and the need to adequately address the surrounding issues of cybersecurity, data protection, protection of privacy and respect for intellectual property rights. It mentions that ICTs shall be used to change gender norms to prevent GBV, report incidents of GBV and coordinate response services.[73] It lacks substantial strategies, however, to regulate the possible cybersecurity issues that can result from the extensive use of ICTs, specifically the challenges of online sexual exploitation and abuse.

Telecommunication Policy, 2004: This Policy aims towards increasing the availability and accessibility of telecommunication services.[74] The Policy explicitly mentions that necessary arrangements, including cyberlaw, shall be made from the collective effort of the concerned ministries, bodies and the private sector.[75] The Policy also mentions that necessary prerequisites shall be built up for the extension of cyberlaw, so that Nepal can enter into the information society.[76]

---

[70] Nepal Telecommunications Authority, *Online Child Safety Directives 2076*, No. 4 (2019).
[71] Ibid., No. 6.
[72] Ibid., No. 23.
[73] Nepal, *National Information and Communication Technology Policy 2072*, sect. 11.4 (2015).
[74] Nepal, *Telecommunication Policy 2060*, sect. 4.1 (2004).
[75] Ibid., sect. 5.7.2.
[76] Ibid., sect. 4.7.

6. SUPPORT SERVICES FOR CHILD VICTIMS AND/OR SURVIVORS OF CYBERCRIME

6.1. *Response mechanisms*

It is obvious that the growing use of technology and information has raised the possibility of online hazards for children and young people. Children are more susceptible to online exploitation because they lack the necessary skills and understanding to use current ICTs safely. Moreover, prior studies have found that it is difficult for the victims of online exploitation to obtain the necessary support services and compensation. The techniques and legal protections that victims of internet exploitation have access to are examined in this section.

According to Article 21 of the Constitution of Nepal (2015), victims of crime have a right to justice, which includes social rehabilitation and compensation. According to article 39(8), every child has the right to child-friendly justice. A child who is a victim of an offence, such as sexual assault or any other type of torture, has the right to seek compensation from the perpetrator, according to article 39(10). Similar to this, section 68 of the Act Relating to Children 2018 mandates that anyone with knowledge of acts of violence or sexual abuse against children that have been, are being, or may be committed should contact the local police department. This includes parents, guardians, teachers, health professionals and anyone else who is taking care of children. Section 74 of the Act states that complaints about an offence punishable under this Act must be filed within the stipulated time limit (if there is one) or within one year after the victim turns 18 years old, whichever comes first. According to section 76, cases involving offences that are punishable under section 66 must be handled as government-party criminal offences.

The Criminal Procedure Code 2017 has provisions for victim and witness protection (section 114). Section 129 mentions the provision of on-camera hearings in sensitive cases like sexual exploitation. The Code also has provisions for fast-track procedures and continuous hearings.

The Crime Victim Protection Act 2018 is dedicated to safeguarding all crime victims, especially children. Some of its most important clauses include the right against discrimination, the right to privacy, the right to information in connection with an investigation, the right to choose a lawyer, the right to compensation, and the right to social rehabilitation.

The ETA is the only specific act in Nepal that deals with crimes committed through electronic means. The ETA is also used when incidents of sexual abuse and exploitation are committed against children through electronic means. Previously, cases of cybercrime used to be prosecuted in Kathmandu District Court only, but after the notice published in the Nepal Gazette on 26 June 2023, cybercrimes are to be investigated by the respective district police offices and prosecuted in the respective district courts.

To raise awareness about cybercrimes and cybersecurity and to investigate such crimes, the Cyber Bureau, a part of Nepal Police, was established in 2018. Although cases of online exploitation are supposed to be investigated and prosecuted in all 77 districts of Nepal, a lack of qualified and competent human resources, financial resources and technologies has yielded

ineffective responses to online crimes, and access to justice for victims of online abuse and exploitation is challenging.[77]

6.2. Support services for the victims of cybercrime

Despite the positive contributions of ICT development and use, the world has also seen the negative effects of ICT misuse. Children and young people have become easy targets for cybercriminals, which is one of the detrimental effects of modern ICTs. Once someone has been mistreated or exploited online, they are constantly at risk of becoming re-victimized. It must be understood that those who have been subjected to internet exploitation require specialized services, support and care. Such circumstances require technological and legal response, as well as victim-focused medical, psychosocial and social treatment. Such kinds of support should take into account the victims'/survivors' overall requirements and should work to establish trust and encouragement to aid them in overcoming feelings of guilt and self-harm. Many parents in Nepal are unaware of the potential threats that children may encounter online. Thus, assistance is also required to help parents comprehend their children's psychological status.[78] A significant number of parents (32.5 per cent) ignored incidents where their children had informed them about online abuses, not responding to such complaints at all.[79]

Support services for children and young people who are victims of cybercrimes are either non-existent or inadequate, as such matters have not been a priority for the government and other duty-bearers. There are considerable gaps in the provision of the following support services:

Medical support: Many people are unclear about the medical care that victims and survivors of internet exploitation need. There is evidence that many offline crimes have an online component. Victims and survivors may require care for their physical as well as emotional health.[80]

Psychosocial support: Most online abuse victims and survivors experience mental discomfort and trauma, which frequently prompts self-harm. To regain their self-confidence and get back to their regular routines, they require psychosocial support.

Legal aid support: From the time the First Information Report is filed until the final court hearing, victims and survivors should receive free legal assistance. They might not understand the legal system and might not be able to afford an attorney.

Technical support: Investigators gather evidence, but victims and survivors may also be required to contribute data in the form of texts, pictures, videos or other kinds of proof. They can lack the technical knowledge needed to provide the necessary data or facts. Therefore, in the context of online abuse, technical help is a crucial part of victim support.

---

[77] Aryal et al., *Internet Safety and Risks of New Technologies.*
[78] UNICEF Innocenti – Global Office of Research and Foresight, *Child Safety Online: Global challenges and strategies*, UNICEF, Florence, Italy, December 2011.
[79] Aryal et al., *Internet Safety and Risks of New Technologies.*
[80] Michigan State University, 'Protecting Yourself from the Latest Internet Sex Crime', phys.org, 21 April 2020, <https://phys.org/news/2020-04-latest-internet-sex-crime.html>, accessed 28 May 2024.

7. SUMMARY OF CHALLENGES AND PROSPECTIVE SOLUTIONS FOR ONLINE CHILD PROTECTION IN NEPAL

7.1.   *Summary of challenges*

A significant proportion of children and young people are accessing the internet regularly without parental guidance. There are several examples of children and young people using the internet without knowing the harm that may result from engaging in risky internet behaviour. Many children are unaware of what constitutes online abuse and exploitation. They do not even know that there is a law in Nepal that criminalizes online abuse. Reports show that since the outbreak of COVID-19, when schools started online classes, children and young people have had more exposure to the internet and are spending more time online than they ever did before. The extended time spent online by children and young people exposes them to a higher risk of online abuse and exploitation. Nepal is benefiting from rapid internet connectivity and increased numbers of users; at the same time, Nepal needs to address the associated threats and vulnerabilities. Children and young people have increased access to new technologies, but they have not been properly informed about the harm that may be caused by the misuse of these technologies. Many parents are unable to monitor and guide their children on the safe use of the internet. Schools do not have curricula for online safety, and teachers are not obliged to teach these issues in schools.

Nepal lacks a comprehensive law against cybercrime, including laws to provide for the online safety of children. Nepal also needs to improve administrative measures, infrastructure, technology and human resources to effectively combat cybercrimes against children and young people.

7.2.   *Prospective solutions*

There is a dire need for the capacity enhancement of law enforcement officials, prosecutors, adjudicators, civil society members and all other relevant stakeholders to combat online child sexual abuse. Additionally, the cross-border nature of cybercrime requires collaborative efforts and cooperation among all stakeholders to establish the foundation for safe and secure internet use. It is the responsibility of the government and the lawmakers, the NTA and the ICT sector, schools and colleges, the media, NGOs and INGOs, and parents and guardians to protect children from online abuse and exploitation.

In December 2014 in London, representatives of countries, leading technology companies and civil society organizations participated in the WeProtect Global Summit to galvanize action against online child sexual exploitation. The result of this summit was the Model National Response (MNR), which supports countries and organizations to prevent and tackle child sexual exploitation and abuse.[81] The MNR has set 21 areas of improvement or intervention.[82]

---

[81] WeProtect Global Alliance, 'The Model National Response', November 2022, <www.weprotect.org/model-national-response/>, accessed 28 May 2024.

[82] Ibid.

The WeProtect Global Alliance and UNICEF conducted a global review on how the MNR is supporting national efforts to end child sexual exploitation and abuse online.[83] The review highlighted the following actions from the Alliance, its members and other stakeholders concerned with protecting children in the digital environment:[84]

- Invest in comprehensive national responses to prevent and respond to online child sexual exploitation and abuse.
- Accelerate global collaboration among governments and companies to strengthen prevention and response efforts to combat online child sexual exploitation and abuse.
- Strengthen the use and collection of data and evidence to enhance effective, sustainable national efforts to protect children.
- Share best practices and lessons learned to support national responses to protect children from online sexual exploitation and abuse.
- Promote the global implementation of the Model National Response framework and its continuous refinement based on lessons learned.

Nepal needs to adopt a national response mechanism, as suggested by the MNR and the global review, and take action accordingly. Moreover, respective stakeholders need to take action, as suggested in the recommendation section below.

---

[83] WeProtect Global Alliance and United Nations Children's Fund, *Framing the Future: How the Model National Response framework is supporting national efforts to end child sexual exploitation and abuse online*, WeProtect Global Alliance, 2022.
[84] Ibid., p. 4.

8. RECOMMENDATIONS AND CONCLUSIONS

8.1. Recommendations

To government/policymakers:

- Develop ICT law as a comprehensive law to address all types of activities that cause victimization of children via misuse of ICTs, and provide definitions of 'child abuse material', 'corruption of children', 'grooming' or 'solicitation of children for sexual purposes', 'sexting', 'sextortion', 'online child sex abuse or livestreaming', 'sex tourism', 'paedophilia' and 'cyberstalking/bullying'.
- Introduce strategies for creating parental-focused policy measures, with an emphasis on raising awareness, creating child-safe zones, providing good internet material and promoting parental controls.
- Take into account the needs, risks and developmental stages of children while formulating policies aimed at protecting children online.
- Develop uniform systems of reporting and complaint handling, and protection systems for victims and witnesses of online sexual exploitation throughout Nepal.
- Incorporate age-appropriate issues of internet safety into school curricula.
- Take effective initiatives to make children and young people aware of the positive and negative aspects of using the internet. Make the internet accessible and affordable across Nepal, making it possible for all to enjoy the various benefits of the internet.
- Take a bottom-up approach to child protection and needs to create interventions from the point of view of children. Online safety of children and young people need to be strictly prioritized by the government.
- Engage, work and develop partnerships with civil societies, the private sector, development sector workers, ISPs and mobile operators, to plan and implement internet ethics to bring about better results.
- Invest in capacity enhancement for investigators, prosecutors, adjudicators and other relevant law enforcement personnel.
- Prioritize and adopt a systematic approach to evidence-based policy development.
- Expand the numbers and scope of hospital-based one-stop crisis management centres to all district hospitals to prevent re-traumatization of victims of online abuse and exploitation.
- Create a dedicated task force comprising representatives from relevant government agencies, NGOs and the private sector to collaboratively address emerging challenges and develop effective solutions.
- Adopt a national response mechanism as suggested by the MNR and the WeProtect Global Alliance/UNICEF 2022 global review and take action accordingly.

To the NTA and the ICT sector:

- Follow the United Nations Guiding Principles on Business and Human Rights, which call on businesses to meet their responsibility to respect children's rights by avoiding any adverse impacts linked to operations, products or services.

- ISPs should report any discoveries of child sexual abuse or child abuse materials to the NTA.
- Develop techniques to restrict searches by implementing a list of prohibited terms, a method increasingly employed by numerous nations. This approach prevents access to websites based on identified phrases within requested URLs. Other similar strategies should also be implemented, such as IP blocking, DNS filtering and URL blocking.
- ISPs should provide information to parents on parental control applications to help them monitor the online activities/behaviours of their children.

To schools and colleges:

- Review the 'history' or browser logs and check files such as cookies, temp history, internet history or cache files, of the school computers to monitor and assess students' online activities.
- Launch internet safety training and internet literacy training for teachers and parents, especially on the linkage between internet use and child marriage.
- Provide awareness of internet safety and online risks in the form of plays, poetry and songs, and provide more practical lessons to students.
- Educate parents and teachers on parental control systems on their mobile phones, computers and other similar devices.
- Schools and colleges should educate children on technical skills for ICT use, but at the same time should also provide a broader understanding of cyber safety.
- Develop complaint-logging mechanisms in schools and colleges if online bullying, exploitation or grooming occurs. Provide professional counselling to students, assuming that children may have a hard time talking/sharing their negative experiences online with their parents and teachers. Counselling can be a good medium to communicate freely without any fear of judgment.
- Introduce e-learning concepts to students to familiarize them with online components of learning.
- Establish counselling services within educational institutions to support children facing online safety issues, ensuring a holistic approach to their well-being.

To media outlets:

- Conduct media literacy programmes and online safety educational campaigns for children and young people. These efforts should be accompanied by public awareness campaigns to better inform parents about the parental control tools at their disposal.
- Develop and promote ethical reporting guidelines for media outlets when covering incidents related to children's online safety, ensuring responsible and non-exploitative reporting.

To NGOs and INGOs:

- Work together for the establishment of effective reporting mechanisms, such as hotlines, 'report abuse' functions and online supports to prevent abusive situations, which can be useful to combat cybercrimes.
- Alert the relevant professionals about the risks of cybercrimes and provide them training on how to recognize warning signs and symptoms of online abuse in children and young people.
- Engage in continuous research to stay abreast of emerging threats and technological developments, and advocate for policies that prioritize the well-being of children in the digital space.
- Provide ongoing training and capacity-building programmes for law enforcement agencies to effectively investigate and address cybercrimes against children.

To parents/guardians:

- Provide adequate and necessary information to children about cyber safety so that they become competent enough to make informed choices, sidestep possible threats and help each other when required.
- Teach children about child-friendly websites and safe internet usage practices, such as keeping online accounts secret, avoiding giving out personal information to strangers online, changing passwords frequently, being cautious when downloading content from the internet, etc. Instruct children to check the authenticity of facts and information provided online.
- Monitor children's online activities.
- Talk and initiate free conversations with children about online risks, such as online harassment and abuse, and guide them towards a better solution, rather than blaming them.
- Encourage positive online behaviours and do not ignore any incidents children share about any problem they have encountered online.
- Recognize children's needs, interests and curiosities while still enforcing rules and time restrictions in an appropriate manner. Apply the 'Don't talk to strangers' rule, as paedophiles and other perpetrators of crimes online frequently pose as youngsters.
- Parents ought to become familiar with computers and the internet. They ought to make use of the parental tools and blocking and filtering services offered by their ISP. Parents who are informed can educate their children about the benefits and drawbacks of ICTs, accessible safety measures, potential sources of assistance and the value of open communication and interaction between parent and child.
- Proactively and regularly access cyber-safety resources designed for parents, to become familiar with emerging technologies and online trends.
- Establish open communication channels between parents, educators and children to facilitate ongoing discussions about online experiences, challenges and concerns.

8.2. Conclusions

The expansion and development of the internet will continue to influence our lives in increasingly significant ways. Developing countries like Nepal will continue to benefit from the rapid global adoption of mobile phone technologies, broadband penetration and online access, as well as the decreasing costs and expanding capacities of these technologies.

As internet access becomes more widespread, children and young people are increasingly exposed to both the benefits and risks associated with online activities. The internet offers enhanced learning opportunities, creative expression and access to a wealth of information and resources that can support educational and personal growth. On the other hand, it also presents significant dangers, including exposure to inappropriate content, cyber-bullying, online predators, and privacy breaches.

Previous studies have shown that children and young people frequently engage in risky online behaviors, such as violating social media rules, sharing personal information and interacting with strangers. Despite the increasing incidence of cybercrimes, Nepal currently lacks the administrative, technological, legal, infrastructural and human resources necessary to effectively address these issues. This gap leaves children and young people vulnerable to various forms of online exploitation and abuse.

The complexity of the digital landscape demands a multifaceted approach to child online protection. Governments must enact and enforce robust laws and regulations that specifically address online safety and the protection of minors. Educational institutions need to incorporate digital literacy and online safety into their curricula to equip young people with the knowledge and skills they need to navigate the internet safely. Parents and guardians also play a crucial role in monitoring and guiding their children's online activities.

Technology companies have a responsibility to design their products and services with child safety in mind. This includes implementing AI-powered content moderation tools to detect and remove harmful content, such as child sexual abuse material and hate speech, before it reaches young users. Additionally, tech companies should prioritize the development of secure platforms that protect users' privacy and personal information.

While protecting children and young people is essential to creating a safer online environment, the government, institutions and corporate sector must ensure that safety is integrated into advocacy for increased access to and the advantages of the internet. Therefore, ccollaboration and cooperation among all stakeholders – including government agencies, law enforcement, technology companies, educational institutions, civil society organizations, parents and children themselves – are essential for creating a safe and protective online environment. Public awareness campaigns can also help educate the broader community about the risks and responsibilities associated with internet use.

The demand for cyber safety must be weighed against the backdrop of evolving technological trends, goods and practices. Cyber safety measures must be flexible and adaptive enough to respond to new opportunities and challenges as they arise, given that technology will continue to become increasingly ingrained in daily life.

To create a protective environment for children in the digital age, it is crucial to foster a culture of continuous learning and adaptation, where policies and practices are regularly reviewed and updated to keep pace with technological advancements and emerging threats. By working together, duty-bearers and stakeholders can create a safer digital environment that allows children and young people to enjoy the benefits of the internet while minimizing the risks. The collaborative effort will lay the foundation for safer and protective online behavior, ensuring that the internet remains a valuable and empowering resource for children and young people.

BIBLIOGRAPHY

1. Allen, Caitlin, 'The Role of the Internet on Sex Trafficking', International Observatory of Human Rights, London, 7 March 2019, <https://iohr.rightsobservatory.org/blog/the-role-of-the-internet-on-sex-trafficking/>, accessed 28 May 2024.

2. Aryal, Kapil, *Assessing and Understanding the Risk: Sexual exploitation of children online in Nepal*, Voice of Children and ECPAT Luxembourg, Kathmandu, 2017.

3. Aryal, Kapil, et al., *Internet Safety and Risks of New Technologies to Children in Nepal*, ECPAT Luxembourg, Kathmandu, December 2019.

4. Barakat, Rahaf, Sameer Abufardeh and Kenneth Magel, 'Automated Framework to Improve Users' Awareness on Online Social Networks', 2016 IEEE International Conference on Electro Information Technology (EIT), Grand Forks, N.D., 19–21 May 2016.

5. Body & Data, *Netizens: Survey on internet usage among urban young people in Nepal*, Body & Data, Bhaktapur, 2021.

6. Child Workers in Nepal and Good Shepherd International Foundation Nepal, *A Study on Online Child Sexual Exploitation in Nepal*, CWIN Nepal, Kathmandu, 2020.

7. Children's Rights Alliance for England, 'Children's Right and Their Online and Digital Interactions: Briefing ahead of Baroness Kidron's debate', CRAE, London, 2014.

8. Dixon, Herbert B., Jr., 'Human Trafficking and the Internet* (*and Other Technologies, Too)', *The Judges' Journal*, vol. 52, no. 1, January 2013.

9. Duncan, Susan Hanley, 'MySpace Is Also Their Space: Ideas for keeping children safe from sexual predators on social networking sites', *Kentucky Law Journal*, vol. 96, no. 4, art. 3, 2008.

10. ECPAT International, *ECPAT Country Overview: Nepal*, ECPAT International, Bangkok, 2020.

11. ECPAT Nepal, 'Sexual Exploitation of Children in Nepal', ECPAT International, Bangkok, 2020.

12. ECPAT Sweden, *Everything That Is Not a Yes Is a No: A report about children's everyday exposure to sexual crimes and their protective strategies*, ECPAT Sweden, Stockholm, 2021.

13. Global Partnership and Fund to End Violence Against Children, *Child Online Safety*, End Violence Against Children, New York, 2022.

14. Government of Nepal Ministry of Communication and Information Technology and Frost & Sullivan, *2019 Digital Nepal Framework: Unlocking Nepal's growth potential,* MoCIT, Kathmandu, 2019.

15. Himalayan News Service, 'Children at High Risk of Sexual Exploitation in Nepal: Report', *The Himalayan Times*, Kathmandu, 2 February 2020, <https://thehimalayantimes.com/nepal/children-at-high-risk-of-sexual-exploitation-in-nepal-report/>, accessed 28 May 2024.

16. Himalayan News Service, 'Cyber Bureau Receives 320 [Com]plaints in Three Months', *The Himalayan Times*, Kathmandu, 27 August 2019, <https://thehimalayantimes.com/kathmandu/cyber-bureau-receives-320-plaints-in-three-months/#:~:text=It%20has%20just%20been%20three,%2C%20Kathmandu%2C%20to%20file%20complaints>, accessed 28 May 2024.

17. Himalayan News Service, 'School Children at High Risk of Online Sexual Abuse', *The Himalayan Times*, Kathmandu, 11 February 2018, <https://thehimalayantimes.com/nepal/schoolchildren-high-risk-online-sexual-abuse/>, accessed 28 May 2024.

18. INHOPE, *Annual Report 2022*, INHOPE, Amsterdam, 2022.

19. International Labour Organization, *Commercial Sexual Exploitation and Trafficking of Children 'In a Nutshell': A resource for Pacific Island countries*, ILO, Geneva, 2015, pp. 30–31.

20. International Telecommunication Union – Development Sector, *Understanding Cybercrime: Phenomena, challenges and legal response*, ITU, Geneva, September 2012.

21. International Trade Union Confederation, Anti-Slavery International and Churches' Commission for Migrants in Europe, *The Role of the Internet in Trafficking for Labour Exploitation*, ITUC, Brussels, 2014.

22. Internet Society, 'Children and the Internet', Internet Society, Geneva, 17 October 2021.

23. Internet Watch Foundation, *The Annual Report 2022: #BehindTheScreens – A deep dive into the digital and social emergency happening*, <https://www.iwf.org.uk/about-us/who-we-are/annual-report-2022/>

24. Internet World Stats, 'Internet Growth Statistics', 2 January 2024, <https://www.statista.com/statistics/617136/digital-population-worldwide/, accessed 28 May 2024>.

25. Kemp, Simon, 'Digital 2023: Nepal', Kepios, 13 February 2023, <https://datareportal.com/reports/digital-2023-nepal>, accessed 28 May 2024.

26. Kostiainen, Mariia, *Internet Safety for Children: Finnish practices and stakeholders*, Master's thesis, University of Tampere – School of Social Sciences and Humanities, April 2016.

27. Merriam-Webster, 'Cybersafety', *Merriam-Webster.com Dictionary*, <www.merriam-webster.com/dictionary/cybersafety>, accessed 28 May 2024.

28. Mitchell, Kimberly J., et al., 'Use of Social Networking Sites in Online Sex Crimes against Minors: An examination of national incidence and means of utilization', *Journal of Adolescent Health*, vol. 47, no. 2, August 2010, pp. 183–190.

29. Mutawa, Noora Al-, Ibrahim Baggili and Andrew Marrington, 'Forensic Analysis of Social Networking Applications on Mobile Devices', *Digital Investigation,* vol. 9, supplement, August 2012, pp. S24–S33.

30. Niroula, Ballav, and Jitendra Prasad Upadhaya, 'Impact of Social Media on the Lifestyle of Youths in Nepal', *Economics and Digital Business Review*, vol. 4, no. 1, 2023, pp. 889–897.

31. Oli, Krishna, 'Child Marriages Increasing in Bajura, Mobiles, Internet Blamed', *República*, Kathmandu, 4 October 2016, <https://myrepublica.nagariknetwork.com/news/child-marriages-increasing-in-bajura-blame-on-phones-internet/>, accessed 28 May 2024.

32. Organization for Economic Co-operation and Development, 'The Protection of Children Online: Risks faced by children online and policies to protect them', *OECD Digital Economy Papers*, No. 179, OECD Publishing, Paris, 2 May 2011.

33. Robinson, Elly, and Vicky Nagy, 'Enhancing Online Safety for Children: Response to the public consultation on key election commitments', Australian Department of Social Services – Australian Institute of Family Studies, Melbourne, March 2014.

34. Setopati, 'Youths More Vulnerable to Cyber Crimes', Lalitpur, 3 February 2019, <https://en.setopati.com/social/138783>, accessed 28 May 2024.

35. Shrestha, Deepesh, and Sadikshya Pradhan, 'Growing Wave of Online Child Sexual Abuse in Nepal: A legal analysis', Forum for Women, Law and Development, Kathmandu, 29 May 2023, <https://fwld.org/wp-content/uploads/2023/05/Growing-Wave-of-Online-Child-Sexual-Abuse-in-Nepal-A-Legal-Analysis-.pdf>, accessed 28 May 2024.

36. Smith, Peter K., Fran Thompson and Julia Davidson, 'Cyber Safety for Adolescent Girls: Bullying, harassment, sexting, pornography, and solicitation', *Current Opinion in Obstetrics and Gynecology*, vol. 26, no. 5, October 2014, pp. 360–365.

37. Telstra Group Limited, *Addressing the Cyber Safety Challenge: From risk to resilience*, Melbourne, July 2014.

38. Thierer, Adam D., 'Rep. Bean's 'Safer Net Act': An education-based approach to online child safety', Progress & Freedom Foundation Progress on Point Paper No. 14.3, Social Science Research Network, 28 March 2007.

39. Third, Amanda, et al., *Young and Online: Children's perspectives on life in the digital age – The State of the World's Children 2017 companion report*, Western Sydney University, Sydney, December 2017.

40. UNICEF Innocenti – Global Office of Research and Foresight, *Child Safety Online: Global challenges and strategies*, UNICEF, Florence, Italy, December 2011.

41. United Nations Children's Fund, *Children's Rights and the Internet: From guidelines to practice – Articles from the Guardian Sustainable Business Child Rights Hub*, UNICEF and *The Guardian*, New York, May 2016.

42. United Nations Entity for Gender Equality and the Empowerment of Women, 'Accelerating Efforts to Tackle Online and Technology Facilitated Violence against Women and Girls (VAWG)', UN Women, January 2022.

43. Voice of Children, *A Study of Situation and Policy Gap Analysis on Online Child Sexual Abuse in Nepal*, Voice of Children, Lalitpur, 2023.

44. Women's Legal and Human Rights Bureau, Inc., 'From Impunity to Justice: Domestic legal remedies for cases of technology-related violence against women', Association for Progressive Communications, 2015.

Annex 1: LIST OF REVIEWED LITERATURE

ARTICLES AND RESEARCH REPORTS

SN	Document Name	Author(s)	Publisher, Year	Link
1.	*Assessing and Understanding the Risk: Sexual exploitation of children online in Nepal*	Kapil Aryal	Voice of Children and ECPAT Luxembourg, 2017	http://ecpat.lu/wp-content/uploads/2018/07/Assessing-Risks-Report-Online-Exploitation-Final.pdf
2.	*Internet Safety and Risks of New Technologies to Children in Nepal*	Kapil Aryal et. al.	ECPAT Luxembourg, 2019	http://ecpat.lu/wp-content/uploads/2020/02/ECPAT-BOOK-Final-book-2020.pdf
3.	'Human Trafficking and the Internet* (*and Other Technologies, Too)'	Herbert B. Dixon Jr.	*The Judges' Journal*, 2013	https://www.americanbar.org/groups/judicial/publications/judges_journal/2013/winter/human_trafficking_and_internet_and_other_technologies_too/
4.	'The Role of the Internet on Sex Trafficking'	Caitlin Allen	International Observatory of Human Rights, 2019	https://iohr.rightsobservatory.org/blog/the-role-of-the-internet-on-sex-trafficking/
5.	'Myspace Is Also Their Space: Ideas for keeping children safe from sexual predators on social-networking sites'	Susan Hanley Duncan	*Kentucky Law Journal*, 2008	https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1296&context=klj
6.	'Use of Social Networking Sites in Online Sex Crimes Against Minors: An examination of national incidence and means of utilization'	Kimberly J. Mitchell et al.	*Journal of Adolescent Health*, 2010	http://unh.edu/ccrc/pdf/CV174.pdf
7.	'Forensic Analysis of Social Networking Applications on Mobile Devices'	Noora Al Mutawa, Ibrahim Baggili and Andrew Marrington	*Digital Investigation*, 2012	https://www.sciencedirect.com/science/article/pii/S1742287612000321
8.	'From Impunity to Justice: Domestic legal remedies for cases of technology-related violence against women'	Women's Legal and Human Rights Bureau, Inc.	Association for Progressive Communications, 2015	https://www.genderit.org/sites/default/files/impunity_womens_legal_dig_0.pdf
9.	'Sexual Exploitation of Children in Nepal'	ECPAT Nepal	ECPAT International, 2020	https://ecpat.org/wp-content/uploads/2021/05/ECPAT-Briefing-Paper-on-the-Sexual-Exploitation-of-Children-in-Nepal-2020-ENG.pdf

10	*ECPAT Country Overview: Nepal*	ECPAT International	ECPAT International, 202	https://ecpat.org/resource/nepal-country-overview/
11	*Understanding Cybercrime: Phenomena, challenges and legal response*	International Telecommunication Union – Development Sector	ITU, 2012	http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
12	'Enhancing Online Safety for Children: Response to the public consultation on key election commitments'	Elly Robinson and Vicky Nagy	Australian Department of Social Services – Australian Institute of Family Studies, 2014	https://aifs.gov.au/research/submissions/enhancing-online-safety-children
13	*Young and Online: Children's perspectives on life in the digital age – The State of the World's Children 2017 companion report*	Amanda Third et al.	Western Sydney University, 2017	https://www.unicef.org/timorleste/reports/young-and-online-childrens-perspectives-life-digital-age
14	*Children's Rights and the Internet: From guidelines to practice – Articles from the Guardian Sustainable Business Child Rights Hub*	United Nations Children's Fund	UNICEF and *The Guardian*, 2016	https://www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf
15	*Child Safety Online: Global challenges and strategies*	UNICEF Innocenti – Global Office of Research and Foresight	UNICEF, 2011	https://digitallibrary.un.org/record/731950?v=pdf
16	*Commercial Sexual Exploitation and Trafficking of Children 'In a Nutshell': A resource for Pacific Island countries*	International Labour Organization	ILO, 2015	https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-suva/documents/publication/wcms_494314.pdf
17	*The Role of the Internet in Trafficking for Labour Exploitation*	International Trade Union Confederation, Anti-Slavery International and Churches' Commission for Migrants in Europe	ITUC, 2014	https://www.ituc-csi.org/IMG/pdf/internet_and_labour_trafficking.pdf
18	'Children and the Internet'	Internet Society	Internet Society, 2021	https://www.internetsociety.org/wp-content/uploads/2017/11/bp-childrenandtheinternet-20129017-en.pdf
19	'The Protection of Children Online:	Organisation for Economic Co-	OECD Publishing, 2011	https://www.oecd-ilibrary.org/docserver/5kgcjf71pl28-

SN	Document Name	Author(s)	Publisher, Year	Link
	Risks faced by children online and policies to protect them'	operation and Development		en.pdf?expires=1596701395&id=id&accname=guest&checksum=E77A4CA5B596ABF84DBA33BA19ECED79

NATIONAL POLICIES

SN	Document Name	Author(s)	Publisher, Year	Link
1.	*2019 Digital Nepal Framework*	Government of Nepal Ministry of Communication and Information Technology and Frost & Sullivan	MoCIT, 2019	https://nepalindata.com/resource/Digital-Nepal-Framework--2019/
2.	National Information and Communication Technology Policy, 2015	Government of Nepal Ministry of Communication and Information Technology	MoCIT, 2015	https://nepalindata.com/resource/NATIONAL-INFORMATION-AND-COMMUNICATION-TECHNOLOGY-POLICY--2015/
3.	Telecommunication Policy, 2060 (2004)	Government of Nepal	Government of Nepal, 2004	http://www.lawcommission.gov.np/en/wp-content/uploads/2018/09/telecommunication-policy-2060-2004.pdf
4.	National Cyber Security Policy	Government of Nepal	Government of Nepal, 2023	https://api.giwms.gov.np/storage/22/posts/1691665949_27.pdf

NATIONAL LAWS

SN	Document Name	Author(s)	Publisher, Year	Link
1.	Constitution of Nepal, 2015	n/a	n/a	https://lawcommission.gov.np/en/wp-content/uploads/2021/01/Constitution-of-Nepal.pdf http://www.lawcommission.gov.np/
2.	Electronic Transaction Act, 2008	n/a	n/a	http://www.tepc.gov.np/uploads/files/12the-electronic-transaction-act55.pdf http://www.lawcommission.gov.np/
3.	Crime Victim Protection Act, 2018	n/a	n/a	https://www.lawcommission.gov.np/en/wp-content/uploads/2019/07/The-Crime-Victim-Protection-Act-2075-2018.pdf
4.	National Criminal Procedure (Code) Act, 2017	n/a	n/a	http://www.moljpa.gov.np/en/wp-content/uploads/2018/12/Criminal-procedure-code-Revised.pdf
5.	Draft Cybercrime Act, 2018	n/a	n/a	https://nta.gov.np/v1/uploads/contents/2017_ITU_Nepal_Draft_Structure_Cybercrime.pdf
6.	Information Technology Bill, 2019	n/a	n/a	http://www.mediapolicy.org.np/nepals-media-policies/
7.	National Penal (Code) Act, 2017	n/a	n/a	https://www.moljpa.gov.np/en/wp-content/uploads/2018/12/Penal-Code-English-Revised
8.	Act Relating to Children, 2018	n/a	n/a	http://www.lawcommission.gov.np/en/wp-content/uploads/2019/07/The-Act-Relating-to-Children-2075-2018.pdf

| 9. | Evidence Act, 1974 | n/a | n/a | http://www.lawcommission.gov.np/en/wp-content/uploads/2018/10/evidence-act-2031-1974.pdf |
| 10. | Cyber Security Bylaw, 2020 | n/a | n/a | https://nta.gov.np/uploads/contents/Cyber-Security-Bylaw-2077-2020.pdf |

MEDIA REPORTS

SN	Document Name	Authors	Publisher, Date	Link
1	'Children Becoming Victims of Sexual Exploitation Due to Internet Misuse'	Rastriya Samachar Samiti	*The Himalayan Times*, 11 February 2021	https://thehimalayantimes.com/kathmandu/children-becoming-victims-of-sexual-exploit-due-to-internet-misuse
2	'How Nepalis' Vulnerability Grows amid Changing Nature of Cyber Crimes'	Anup Ojha	*The Kathmandu Post*, 14 May 2023	https://kathmandupost.com/national/2023/05/14/how-nepalis-vulnerability-grows-amid-changing-nature-of-cyber-crimes
3	'Nepal Not Doing Enough to Tackle Online Child Abuse'	Anup Ojha	*The Kathmandu Post*, 9 June 2023	https://kathmandupost.com/national/2023/06/09/nepal-not-doing-enough-to-tackle-online-child-abuse
4	'How Loot Boxes in Children's Video Games Encourage Gambling'	Jason W. Osborne	*Forbes*, 25 May 2023	https://www.forbes.com/sites/jasonwosborne/2023/05/25/how-loot-boxes-in-childrens-video-games-encourage-gambling/
5	'Shallow Fakes Tell Half-Truths'	Aishwarya Baidar	The Record, 23 April 2021	https://www.recordnepal.com/shallow-fakes-tell-half-truths
6	'How TikTok's Algorithm 'Exploits the Vulnerability' of Children'	Kevin Rawlinson	*The Guardian*, 4 April 2023	https://www.theguardian.com/technology/2023/apr/04/how-tiktoks-algorithm-exploits-the-vulnerability-of-children
7	'TikTok Fined £12.7m for Illegally Processing Children's Data'	Alex Hern and Aletha Adu	*The Guardian*, 4 April 2023	https://www.theguardian.com/technology/2023/apr/04/tiktok-fined-uk-data-protection-law-breaches
8	'Sharing Photos of Your Kids? Maybe Not after You Watch This Deepfake Ad'	Emmanuelle Saliba	ABC News, 28 July 2023	https://abcnews.go.com/GMA/Family/sharing-photos-kids-after-watch-deepfake-ad/story?id=101730561
9	'Father Warns Others about AI Voice Scams after His Family Lost $1k'	Anthony McMahon and Sean Sanders	*Good Morning American*, 16 May 2023	https://www.goodmorningamerica.com/news/story/dad-warns-ai-voice-scams-after-family-lost-99344931
10	'Social Media Addiction among Nepali Children Adds to Security and Health Worries'	Monica Lohani	Nepal Minute, 14 July 2022	https://www.nepalminute.com/detail/82/social-media-addiction-among-nepali-children-adds-to-security-and-health-worries

11	'Addressing Gender Violence in Cyberspace'	Prashansha Rimal	The Record, 24 March 2022	https://www.recordnepal.com/addressing-gender-violence-in-the-cyberspace
12	'Nepal Police Calms Fears over Escalating AI-Based Cybercrimes'	Diwash Ghimire	Nepal Minute, 11 January 2023	https://www.nepalminute.com/detail/1584/nepal-police-calms-fears-over-escalating-ai-based-cybercrimes
13	'ChatGPT, a Terror Factor or Teaching Tool?'	Diwash Ghimire	Nepal Minute, 4 February 2023	https://www.nepalminute.com/detail/1746/chatgpt-a-terror-factor-or-teaching-tool-2023-Feb-03-409200
14	'Acting Together to End Gender-Based Violence'	Ambassadors and representatives of I/NGOs	*The Kathmandu Post*, 24 November 2022	https://kathmandupost.com/columns/2022/11/24/acting-together-to-end-gender-based-violence#:~:text=Gender%2Dbased%20violence%20(GBV),achieve%20sustainable%20development%20for%20all.
15	'Govt Approves National Cyber Security Policy 2023'	República	*República*, 9 August 2023	https://myrepublica.nagariknetwork.com/news/govt-approves-national-cyber-security-policy-2023/
16	'Child Marriage in Nepal Today is More Voluntary than Forced. What Are Its Implications?'	Nasana Bajracharya	OnlineKhabar, 19 December 2022	https://english.onlinekhabar.com/early-marriage-child-marriage-nepal.html
17	'Cyberbullying: Let's talk about this'	Aashika Shrestha	NepalNews, 17 January 2022	https://nepalnews.com/s/issues/cyberbullying-let-s-talk-about-this
18	'Pedophiles Using Open-Source AI to Create Child Sexual Abuse Content, Says Watchdog'	Dan Milmo	*The Guardian*, 13 September 2023	https://www.theguardian.com/society/2023/sep/12/paedophiles-using-open-source-ai-to-create-child-sexual-abuse-content-says-watchdog#:~:text=Freely%20available%20artificial%20intelligence%20software,victims%20to%20create%20new%20content
19	'Youths more Vulnerable to Cyber Crimes'	Setopati	Setopati, 3 February 2019	https://en.setopati.com/social/138783
20	'Schoolchildren at High Risk of Online Sexual Abuse'	Himalayan News Service	*The Himalayan Times*, 11 February 2018	https://thehimalayantimes.com/nepal/schoolchildren-high-risk-online-sexual-abuse/
21	'Cyber Bureau Receives 320 [Com]plaints in Three Months'	Himalayan News Service	*The Himalayan Times*, 27 August 2019	https://thehimalayantimes.com/kathmandu/cyber-bureau-receives-320-plaints-in-three-months/#:~:text=It%20has%20just%20been%20three,%2C%20Kathmandu%2C%20to%20file%20complaints.
22	'Children at High Risk of Sexual Exploitation in Nepal: Report'	Himalayan News Service	*The Himalayan Times*, 2 February 2020	https://thehimalayantimes.com/nepal/children-at-high-risk-of-sexual-exploitation-in-nepal-report/

| 23 | 'Child Marriages Increasing in Bajura, Mobiles, Internet Blamed' | Krishna Oli | *República*, 4 October 2016 | https://myrepublica.nagariknetwork.com/news/child-marriages-increasing-in-bajura-blame-on-phones-internet/ |

Annex 2: ORGANIZATIONS WORKING ON THE ONLINE SAFETY OF CHILDREN AND YOUNG PEOPLE

SN	Organization	Key Initiatives
1.	ChildSafeNet (www.childsafenet.org)	ChildSafeNet is the only organization 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 the organization's main programme activities. ChildSafeNet has conducted a number of research studies and surveys on online protection of children and young people, including research studies on children's and young people's online behaviours and risks (2018–2019), research studies on the livestreaming of sexual abuse and exploitation of children and young people (2020), and a survey on COVID-19 and its impacts on the protection of children and young people online (2020). ChildSafeNet has worked with UNICEF Nepal to develop a situation paper on cyber safety for children and young people in Nepal. The organization has conducted a desktop review of over 160 documents (research reports, policies, laws, technical papers and other relevant documents); prepared a technical note on COVID-19 and the protection of children and young people online; and developed four toolkits (for police, lawyers, psychosocial service providers and parents), a cyber safety booklet, and a detailed FAQ. ChildSafeNet has developed offline and online training modules on cyber safety. Every year, the organization conducts cyber safety 'training of trainers' sessions and has so far produced more than 60 trainers. ChildSafeNet's trainings have benefited more than 4,000 children, young people and parents. ChildSafeNet has produced video PSAs, digital posters, articles and blogs on cyber safety to raise awareness, and

		has been organizing Safer Internet Day (www.saferinternetday.org) in Nepal since 2019.
2.	Child Workers in Nepal (CWIN) (www.cwin.org.np)	Child Workers in Nepal (CWIN) is a leading child rights organization in Nepal. CWIN conducted a research study on internet safety of children in 2008 and a study on online child sexual exploitation in Nepal in 2020. The organization has produced video and print awareness materials on internet safety
3.	ECPAT Luxembourg (www.ecpat.lu)	ECPAT Luxembourg collaborated with Voice of Children to raise awareness on cyber safety and conduct research on online sexual exploitation of children in 2017. ECPAT Luxembourg also conducted a research study on online safety in 2019. The organization collaborated with ChildSafeNet in 2020 to conduct a rapid assessment of research on livestreaming of sexual abuse and exploitation of children and young people in Nepal. ECPAT Luxembourg has provided support to the Central Cyber Bureau of Nepal Police on awareness raising.
4.	Center for Legal Research and Resource Development (CeLRRd) (https://celrrd.org/)	Since its inception in 1998, the Center for Legal Research and Resource Development (CeLRRd) has worked extensively to promote, uphold and respect rule of law, good governance, fair and unrestricted access to justice, human rights and peace. To date, it has distinguished itself among other Nepalese NGOs for its high-calibre legal research and for its unparalleled development of domestic legal resources. CeLRRd has performed research and held seminars for children's internet safety and rights. For the protection of children online, CeLRRd has concentrated on legislative change and engagement with hotel, travel and tour operators, as well as internet service providers. CeLRRd also provides free legal aid to child victims of online abuse and exploitation.
5.	Voice of Children (www.voiceofchildren.org.np)	Voice of Children conducted awareness-raising activities and a research study on cyber safety of children, in collaboration with ECPAT Luxembourg. The organization has produced radio and TV programmes on cyber safety for children and has also produced IEC materials.
6.	SathSath (www.sathsath.org)	SathSath has conducted cyber safety awareness activities focused on the sexual abuse and exploitation of boys. The organization has produced IEC materials on cyber safety.
7.	UNICEF Nepal (www.unicef.org/nepal/)	UNICEF Nepal has conducted cyber safety awareness activities under its Net4Good programme. The organization has produced video and print IEC materials and has provided support to the CSOs for conducting cyber safety training.

		UNICEF has partnered with ChildSafeNet to develop a situation 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 also supported the development of toolkits and other resources.
8.	Terres des Hommes Netherlands (www.terredeshommes.nl/en)	Children are the focus of the mission, vision and values because they are part of the present and represent the future. The world holds many threats: poverty, epidemics, armed conflicts, natural disasters, the climate emergency, and so on, and children and young people are at the front line of greatest exposure to those dangers. They are entitled to be protected, supported and heard.
9.	Good Shepherd International Foundation Nepal (GSIF Nepal) (https://www.gsif.it/countries/nepal/)	The Good Shepherd International Foundation works for the welfare of girls, women and children, especially those who live in poverty and are affected by violence, abuse and discrimination.
10.	Saathi (www.saathi.org.np)	Saathi is a non-governmental organization established in 1992 to address the different forms of violence and discrimination faced by Nepalese women and girls. It has been drawing significant national attention towards domestic violence in Nepal as an area requiring urgent attention and intervention to break the silence that impacts the lives of many marginalized women and girls.
11.	Net4Good Alliance (https://net4goodalliance.com/)	Net4Good Alliance is a national-level loose network formed in January 2022 by organizations working in the field of child rights and child online safety, aiming to work closely with government entities, the private sector and related stakeholders to ensure child online safety.
12.	BlinkNow Foundation (https://blinknow.org/)	BlinkNow Foundation works to empower Nepal's children by providing quality education and a safe environment, and through inspiring others.
13.	Forum for Digital Equality/Child Safety Initiative (https://digitalequality.org.np/)	Online Child Safety Initiative is a consortium initiative to protect against online child abuse, led by the Forum for Digital Equality. In particular, the platform aims at encouraging reporting of child abuse imagery content through a portal. This initiative also provides support on psychosocial counseling, technical and legal assistance for online child abuse cases.
14.	Loom Nepal (www.taannepal.org.np)	Loom Nepal is a feminist platform that recognizes the diversity and intersectionality of women in Nepal and collaboratively engages to dismantle the power hierarchy, sustain activism and reimagine the feminist movement. Loom works towards harnessing the collective power of women through multigenerational activism, where activists across ages and experiences connect, organize and transform structures that obstruct their equality.

15.	Women Youth Empowerment in Social Service and Human Rights (WYESHR) (https://www.wyeshr.org/)	Women Youth Empowerment in Social Service and Human Rights (WYESHR) is a non-profit organization that works as the leading female and survivor-led development agency. WYESHR has worked with the community spheres for combatting trafficking, supporting protection, prevention and prosecution, and advocating for the human rights of survivors and victims of commercial and non-commercial trafficking and the adult entertainment sector.
16.	Digital Rights Nepal (DRN) (www.digitalrightsnepal.org)	Digital Rights Nepal (DRN) is a not-for-profit initiative dedicated to the protection and promotion of digital rights in Nepal. DRN has been fostering collaboration with concerned agencies including CSOs and government bodies to build synergy and solidarity in addressing the issues related to online child protection. It has organized online campaigns and awareness-raising events targeted to students and youths to promote online safety and security awareness.

Back Cover (Inside)

ChildSafeNet

ChildSafeNet is a non-profit organization established with the mission to promote a safer and better internet. We work to protect children and young people from online sexual abuse and exploitation, cyber-bullying, phishing, gaming and screen addiction. We advocate for a protective environment for children in the digital age, safeguarding their right to be protected both online and offline.

Jawalakhel, Lalitpur, Nepal
Tel: +977 9741673313
Email: info@childsafenet.org
Website: www.childsafenet.org

unicef ⊕ | for every child

UNICEF is mandated by the United Nations General Assembly to advocate for the protection of children's rights, to help meet their basic needs and to expand their opportunities to reach their full potential. We are guided by the Convention on the Rights of the Child and strive to establish children's rights as enduring ethical principles and international standards of behavior towards children.

Pulchowk, Lalitpur, Nepal
Tel: +977 1 5523200
Email: kathmandu@unicef.org
Website: www.unicef.org/nepal