ITU Publications

International Telecommunication Union
Development sector

Guidelines for policy-makers on Child Online Protection

2020

Guidelines for policy-makers on Child Online Protection

2020

Acknowledgements

These guidelines have been developed by the International Telecommunication Union (ITU) and a working group of contributing authors from leading institutions active in the sector of information and communication technologies (ICT) as well as in child (online) protection issues and included the following organisations:

ECPAT International, Global Kids Online network, the Global Partnership to End Violence Against Children, project HABLATAM, Insafe network of Safer Internet Centres (Insafe), INTERPOL, the International Centre for Missing & Exploited Children (ICMEC), the International Disability Alliance, the International Telecommunications Union (ITU), the Internet Watch Foundation (IWF), the London School of Economics, the Office of the Special Representative of the Secretary-General on Violence against Children and the Special Rapporteur on the sale and sexual exploitation of children, Privately SA, RNW Media, UK Safer Internet Centres, the WePROTECT Global Alliance (WPGA) and the World Childhood Foundation USA.

The working group was chaired by David Wright (UK Safer Internet Centres/SWGfL) and coordinated by Fanny Rotino (ITU).

These guidelines would not have been possible without the time, enthusiasm and dedication of the contributing authors. Invaluable contributions were also received by the COFACE-Families Europe, the Council of Europe, Australian eSafety Commissioner, the European Commission, the e-Worldwide Group (e-WWG), the OECD, Youth and Media at the Berkman Klein Center for Internet and Society at Harvard University as well as individual national governments and industry stakeholders that share a common objective of making the Internet a better and safer place for children and young people.

ITU is grateful to the following partners, who have contributed their valuable time and insights: (listed in alphabetical order of organisation):

- Martin Schmalzried (COFACE-Families Europe)
- Livia Stoica (Council of Europe)
- John Carr (ECPAT International)
- Julia Fossi and Ella Serry (eSafety Commissioner)
- Manuela Marta (European Commission)
- Salma Abbasi (e-WWG)
- Amy Crocker and Serena Tommasino (Global Partnership to End Violence Against Children)
- Lionel Brossi (HABLATAM)
- Sandra Marchenko (ICMEC)
- Karl Hopwood (Insafe)[1]
- Lucy Richardson (International Disability Alliance)
- Matthew Dompier (Interpol)
- Fanny Rotino (ITU)
- Tess Leyland (IWF)
- Sonia Livingstone (London School of Economics & Global Kids Online)

[1] *Under the Connecting Europe Facility (CEF), European Schoolnet runs, on behalf of the European Commission, the Better Internet for Kids platform, which includes the coordination of the Insafe network of European Safer Internet Centres. More information is available at* www.betterinternetforkids.eu

- Elettra Ronchi (OECD)
- Manus De Barra (Office of the Special Representative of the Secretary-General on Violence against Children)
- Deepak Tewari (Privately SA)
- Pavithra Ram (RNW Media)
- Maud De Boer-Buquicchio (United Nations Special Rapporteur on the sale and sexual exploitation of children)
- David Wright (UK Safer Internet Centres/SWGfL)
- Iain Drennan and Susannah Richmond (WePROTECT Global Alliance)
- Lina Fernandez and Dr. Joanna Rubinstein (World Childhood Foundation USA)
- Sandra Cortesi (Youth and Media)

ISBN

978-92-61-30121-7 (Paper version)

978-92-61-30451-5 (Electronic version)

978-92-61-30111-8 (EPUB version)

978-92-61-30461-4 (Mobi version)

Please consider the environment before printing this report.

Foreword

In a world where the Internet permeates almost every aspect of modern life, keeping young users safe online has emerged as an increasingly urgent issue for every country.

ITU developed its very first set of Child Online Protection Guidelines way back in 2009. Since those early days, the Internet has evolved beyond all recognition. While it has become an infinitely richer resource for children to play and learn, it has also become a much more dangerous place for them to venture unaccompanied.

From issues of privacy to violent and inappropriate content, to Internet scammers and the spectre of online grooming, sexual abuse and exploitation, today's children face many risks. Threats are multiplying, and perpetrators increasingly operate simultaneously across many different legal jurisdictions, limiting the effectiveness of country-specific responses and redress.

In addition, the COVID-19 global pandemic saw a surge in the number of children joining the online world for the first time, to support their studies and maintain social interaction. The constraints imposed by the virus not only meant that many younger children began interacting online much earlier than their parents might have planned, but the need to juggle work commitments left many parents unable to supervise their children, leaving young people at risk of accessing inappropriate content or being targeted by criminals in the production of child sexual abuse material.

More than at any time before, keeping children safe online requires a collaborative and coordinated international response, demanding the active involvement and support of a broad number of stakeholders – from industry stakeholders including private sector platforms, service providers and network operators, to governments and civil society.

Recognizing this, in 2018 ITU Member States requested something more than the timely refresh of the COP Guidelines that has been undertaken periodically in the past. Instead, these new revised guidelines have been re-thought, re-written and re-designed from the ground up to reflect the very significant shifts in the digital landscape in which children find themselves.

In addition to responding to new developments in digital technologies and platforms, this new edition addresses an important lacuna: the situation faced by children with disabilities, for whom the online world offers a particularly crucial lifeline to full – and fulfilling – social participation. Consideration of the special needs of migrant children and other vulnerable groups has also been included.

For policy-makers, we hope these guidelines will serve as a solid foundation on which to develop inclusive, multi-stakeholder national strategies, including open consultations and dialogues with children, to develop better-targeted measures and more efficient actions.

In developing these new guidelines, ITU and its partners sought to create a highly usable, flexible and adaptable framework firmly based on international standards and shared goals – particularly the Convention on the Rights of the Child and the UN Sustainable Development Goals. In the true spirit of the ITU role as a global convener, I am proud of the fact that these revised guidelines are the product of a global collaborative effort and are co-authored by international experts drawn from a broad multi-stakeholder community.

I'm also delighted to introduce our new COP mascot, Sango, a friendly, feisty and fearless character designed entirely by a group of children, as part of the new ITU international youth outreach programme.

In an age where more and more young people are coming online, these COP Guidelines are more vital than ever. Policy-makers, industry, parents and educators – and children themselves – all have a vital role to play. I am grateful, as always, for your support, and I look forward to continuing our close collaboration on this critical issue.

Doreen Bogdan-Martin
Director, Telecommunication Development Bureau

Preface

Thirty years ago, nearly all governments pledged to respect, protect and promote children's rights. The UN Convention on the Rights of the Child (CRC) is the most widely ratified international human rights treaty in history. While notable progress has been achieved in the past three decades, significant challenges remain and new areas of risks for children have emerged.

In 2015, all nations renewed their commitment to children to the 2030 agenda and the 17 universal Sustainable Development Goals (SDGs). Goal 16.2 for instance calls for an end to abuse, exploitation and all forms of violence and torture against children by 2030. But protecting children is a common thread within 11 of the 17 SDGs. UNICEF puts children at the centre of the 2030 agenda as depicted in Figure 1.

Figure 1: Children, ICTs, and SDGs

The 2030 Agenda for Sustainable Development recognizes that ICTs can be a key enabler to attain the SDGs. The spread of information and communication technology (ICTs) and global interconnectedness has the potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies. It further defines specific targets for the use of ICTs for sustainable development in education (Goal 4), gender equality (Goal 5), infrastructure (Goal 9 – universal and affordable access to the Internet) and Goal 17 – partnerships and means of implementation[1]. ICT has the power to deeply transform the economy as a whole by being a driving force in achieving each and every one of the 17 SDGs. ICTs have already made their move by empowering billions of individuals around the world – by providing access to education resources and healthcare, and services such as e-government and social media, among others.

The explosion of information and communication technology has herewith created unprecedented opportunities for children and young people to communicate, connect, share, learn, access information and express their opinions on matters that affect their lives and their communities.

But wider and more easily available access to the Internet and mobile technology also poses significant challenges to children's safety and wellbeing – both online and offline.

---

[1] UNDP, Sustainable Development Goals | UNDP, undp.org, accessed January 29, 2020, https://www.undp.org/content/undp/en/home/sustainable-development-goals.html; Houlin Zhao, "Why ICTs Are so Crucial to Achieving the SDGs," *ITU*, ITU News Magazines, 48, accessed January 29, 2020, https://www.itu.int/en/itunews/Documents/2017/2017-03/2017_ITUNews03-en.pdf.

To reduce the risks of the digital world while enabling more children and young people to reap its benefits, governments, civil society, local communities, international organizations and industry must come together in common purpose. Policy-makers in particular are needed in order to achieve an international goal to keep children safe online.

In order to respond to the challenges posed by the rapid development of ICTs and the child protection challenges they bring, the Child Online Protection (COP) Initiative was launched as a multi-stakeholder international initiative by the International Telecommunication Union (ITU) in November 2008. This initiative aims to bring together partners from all sectors of the global community to create a safe and empowering online experience for children around the world.

Moreover, the Plenipotentiary Conference of the International Telecommunication Union held in Dubai in 2018, reaffirmed the importance of the COP Initiative by acknowledging it as a platform to raise awareness, share best practices, and to provide assistance and support to Member States, especially developing countries, in developing and implementing COP roadmaps. It also recognised the importance of the protection of children online within the framework of the United Nations Convention on the Rights of the Child and other human rights treaties by encouraging collaboration between all stakeholders involved in child online protection.

The Conference recognized the 2030 Agenda for Sustainable Development, addressing various aspects of child online protection in the Sustainable Development Goals (SDGs), in particular SDGs 1, 3, 4, 5, 9, 10 and 16; it further recognized Resolution 175 (Rev. Dubai, 2018), on accessibility for persons with disabilities and persons with specific needs to telecommunication/ information and communication technology (ICT) and Resolution 67 (Rev. Buenos Aires, 2017) of the World Telecommunication Development Conference (WTDC), on the role of the ITU Telecommunication Development Sector (ITU-D) in child online protection.

In late 2019, ITU/UNESCO Broadband Commission for Sustainable Development launched the Child Online Safety Report with actionable recommendations on how to make the Internet safer for children.

In 2009, the first set of guidelines on child online protection were issued by ITU in the context of the COP Initiative. Over the last decade, the COP Guidelines have been translated into many languages and have been used by many countries in the world as a reference point for road maps and national strategies related to child online protection. They have served national government entities, civil society organizations, childcare institutions, industry and many other stakeholders in their child online protection efforts.

More specifically, the guidelines have been used for the draft, development and implementation of national child online protection strategies in many Member States such as Cameroon, Gabon, Gambia, Ghana Kenya, Sierra Leona, Uganda, and Zambia in the Africa region; Bahrain and Oman in the Arab region; Brunei, Cambodia Kiribati, Indonesia, Malaysia, Myanmar and Vanuatu in Asia Pacific region; and Bosnia, Georgia, Moldova, Montenegro, Poland and Ukraine in the Europe region.

Furthermore, the guidelines have built the foundation for regional events such as the Regional Conference on Child Online Protection (ACOP): Empowering the Future Digital citizens, in Kampala, Uganda (2014), and the ASEAN Regional Conference on Child Online Protection held in Bangkok, Thailand (2020).

According to Resolution 179 (Rev. Dubai, 2018), ITU in collaboration with COP initiative partners and stakeholders has been instructed to update the four sets of guidelines taking into consideration technology developments in the telecommunication industry, including guidelines on children with disabilities and children with specific needs.

As a result of this process, these guidelines have been significantly updated and reviewed by experts and relevant stakeholders, establishing a broad set of recommendations to keep children safe in the digital world. They are the result of a collaborative multi-stakeholder effort, tapping into the knowledge, experience and expertise of many organizations and individuals from across the world in the field of child online protection. They aim to establish the foundations for a safe and secure cyber world for future generations. They are meant to act as a blueprint, which can be adapted and used in a way that is consistent with national or local customs and laws. Moreover, these guidelines address issues which affect all children and young people under the age of 18, recognising the different needs of each age group. They furthermore aim to address the needs of children in different living conditions and children with special needs and disabilities. The guidelines also strengthen the scope of child online protection, addressing all risks, threats and harms that children may encounter online and to balance these carefully with the benefits the digital world can bring to children's lives.

It is hoped that these guidelines will not only lead to the building of a more inclusive information society, but also enable ITU Member States to meet their obligations towards protecting and realizing the rights of children as laid out in the UN Convention on the Rights of the Child[2], adopted by UN General Assembly resolution 44/25 of 20 November 1989 and the World Summit on Information Society[3] (WSIS) Outcomes Document.

Through issuing these guidelines, the COP initiative calls upon all stakeholders to implement policies and strategies that will protect children in cyberspace and promote their safer access to all the extraordinary opportunities online resources can provide.

---

2 UNICEF, "Convention on the Rights of the Child," uncief.org, accessed January 29, 2020, https://www.unicef.org/child-rights-convention.

3 WSIS was held in two phases: in Geneva (10-12 December 2003) and in Tunis (16-18 November 2005). WSIS concluded with a bold commitment "to build a people-centered, inclusive and development-oriented information society, where everyone can create, access, utilize and share information and knowledge."

Table of Contents

List of tables, figures and boxes

Tables

Figures

Boxes

1. Document overview

1.1 Purpose

National governments have an obligation to provide for the protection of children in both the physical and virtual worlds. In an important sense, because the new technologies are now so thoroughly integrated into the lives of so many children and young people in a number of important ways, it no longer makes sense to try to maintain rigid distinctions between real world events and online events. The two are increasingly intertwined and interdependent.

Policy-makers[1] and all other relevant stakeholders have very important roles to play. The speed by which technology is evolving means that many of the traditional methods of policy-making no longer fit this purpose. Policy-makers are required to elaborate a legal framework that is adaptive, inclusive, and fit for purpose for the fast-changing digital age to protect children online.

The purpose of these guidelines is to offer policy-makers in ITU Member States a user-friendly and flexible framework to understand and act upon their legal obligation to provide for the protection of children in both the real, physical and virtual worlds.

The guidelines do this by addressing several important questions for policy-makers:

1) What is child online protection?
2) Why do I as a policy-maker need to care about child online protection?
3) What is the legal, socio-political, and development context of my country?
4) How should policy-makers start to consider and shape an effective and sustainable child online protection policy in their country?

In so doing, the guidelines draw upon existing models, frameworks and resources to offer context and insight into good practice from across the world.

1.2 Scope

The scope of child online protection extends to any harm that children are exposed to online, covering a broad range of risks that threaten the safety and wellbeing of children. It is a complex challenge that must be approached from multiple angles, including legislation, governance, education, policy and society.

In addition, child online protection must be based on an understanding of both general and country-specific risks, threats and harms facing children in digital environments. This requires clear definitions and the establishment of clear parameters for intervention that include and differentiate between acts constituting a crime and those that while not illegal, nevertheless pose a threat to the wellbeing of a child.

To this end, the guidelines provide an overview of the current threats and harms facing children in digital environments. That said, the speed at which the technology and associated threats and harms are evolving means that the traditional speed and method of policymaking is unable to keep pace. Policy-makers in the digital age need to build legal and policy frameworks that are

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

adaptive and inclusive enough to tackle existing challenges and as far as possible anticipate those to come. Doing this requires collaboration with each and every stakeholder, including the ICT industry, the research community, civil society, the public, and children themselves. This process can be supported by consideration of overarching principles in child online protection.

1.3 Overarching principles

Eleven cross-cutting principles set out here, which taken together, will help in the development of a forward-looking and holistic national child online protection strategy.

The order of these principles reflects a logical narrative rather than an order of importance.

A national child online protection strategy should:

1. be based on a holistic vision that incorporates government, industry, and society;
2. result from an all-encompassing understanding and analysis of the overall digital environment yet be tailored to the country's circumstances and priorities;
3. respect and be consistent with the fundamental rights of children as enshrined in the UN Convention on the Rights of the Child and other key international conventions and laws;
4. respect and be consistent with existing, similar and related domestic laws and strategies in place such as child abuse laws or child safety strategies;
5. respect children's civil rights and freedoms, which should not be sacrificed to protection;
6. be developed with the active participation of all relevant stakeholders including children, addressing their needs and responsibilities and meeting the needs of minority and marginalised groups;
7. be designed to align with broader government plans for economic and social prosperity and maximise the contribution of ICTs to sustainable development and social inclusion;
8. utilise the most appropriate policy instruments available to realise its objective, considering the country's specific circumstances;
9. be set at the highest level of government, which will be responsible for assigning relevant roles and responsibilities and allocating sufficient human and financial resources;
10. help build a digital environment that children, parents/caregivers and stakeholders can trust;
11. guide efforts of stakeholders to empower and educate children on digital literacy to protect themselves online.

1.4 Usage of these guidelines

These guidelines consider the relevant research, existing models and material, and set out clear recommendations for the development of a national child online protection strategy.

- Section 2 introduces child online protection and gives insights into recent research including aspects regarding new emerging technologies, key threats and harms for children.
- Section 3 sets out how to prepare for a national child online protection strategy, including relevant stakeholders, existing examples of responses to online threats and harms and benefits of having a national strategy.
- Section 4 covers recommendations for frameworks and implementation.
- Section 5 outlines national checklists to develop a national child online protection strategy.
- Section 6 gives useful reference materials.

2. Introduction

In 2019, more than half of the world's population used the Internet. The largest group of users are those aged under 44, with use equally high among 16 to 24-year-olds and 35 to 44-year-olds. At the global level, one in three children use the Internet (0-18 years)[2]. In developing countries, children and young people are leading Internet usage[3], and it is estimated that over the next five years, this population will more than double. New generations are growing up with the Internet and most are connecting with mobile network technology, especially in the global south[4].

Though Internet access is fundamental to the realization of children's rights, there are still significant regional, national, gender and other disparities of access that limit the opportunities for girls, children with disabilities, children from minorities and other vulnerable groups. In terms of digital gender divide, research shows that in every region except the United States of America, male Internet users largely outnumber female users. In many countries, girls do not have the same access opportunities as boys, and where they do, girls are not only monitored and restricted in their Internet usage to a much greater extent, but they may also find their safety at risk in efforts to access the Internet[5]. It is clear that children and young people who lack digital skills or speak minority languages cannot easily find relevant content online, and that children from rural areas have fewer digital skills, spend more time online (especially playing games), and receive less parental mediation and monitoring[6].

However, no conversation about risks and threats can take place without acknowledging the tremendously enriching and empowering nature of digital technology. The Internet and digital technologies are transforming the way we live and have opened up many new ways to communicate, play games, enjoy music and engage in a vast array of cultural, educational and skill-enhancing activities. The Internet can provide crucial access to health and educational services as well as information on topics that are important for young people but may be taboo in their societies.

Just as children and young people are often at the forefront of adopting and adapting to the new possibilities provided by the Internet, they are also being exposed to a range of safety and welfare-related issues that must be acknowledged and confronted by society. It is essential to discuss openly the risks that exist for children and young people online. Discussion opens up a platform from where children and young people can be taught how to recognise risk, and

---

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

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

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

5 "Young Adolescents and Digital Media: Uses, Risks and Opportunities in Low-and Middle-Income Countries,"GAGE, accessed January 29, 2020,https://www.gage.odi.org/publication/digital-media-risks-opportunities/.

6 Livingstone, S., Kardefelt Winther, D., and Hussein, M. (2019). *Global Kids Online Comparative Report, Innocenti Research Report*. UNICEF Office of Research - Innocenti, Florence, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html. This can have unexpected results, for example, research undertaken by HABLATAM in five Latin American countries has shown that in vulnerable communities, children may be using dating platforms, videogames, and social networks to perform money transactions for illegal purposes. Contectados al Sur network, "Hablatam," Hablatam Project 2020, accessed February 6, 2020, https://hablatam.net/.

prevent or deal with harms should they materialize, as well as the advantages and opportunities the Internet can offer.

In many parts of the world, young people have a good understanding of some of the risks they face online.[7][8] Research has shown, for example that the majority of children and young people are able to distinguish cyberbullying from joking or teasing online. They recognise that cyberbullying has a public dimension and is designed to harm, yet balancing a child's online opportunities and risks remains a challenge[9].

For ITU Member States, protecting children and young people online continues to be a priority, that it must be carefully balanced with efforts to promote opportunities for children and young people online[10], and that it must be done in a way that protects children and young people without affecting their access or the wider public's access to information, or the ability to enjoy freedom of speech, expression and association.

There is an obvious need for dedicated investment and creative solutions to address the risks faced by children and young people, not least because of the digital divide between children and adults that limits guidance from parents, teachers, and guardians. At the same time, as children and young people grow up and become adults, parents and active members of society, there is a potential and unmissable opportunity for them to reduce the digital divide.

In light of this, building trust in the Internet must be at the front and centre of public policy. Governments and society need to work with children and young people to understand their perspectives and spark genuine public debate about risks and opportunities. Supporting children and young people to manage online risks can be effective, but governments must also ensure that there are adequate support services for those who experience harm online, and that children are aware of how to access those services.

Some countries struggle to allocate sufficient resources to tackle digital literacy and safety of children online. However, children report that parents, teachers, technology companies, and governments are important players in developing solutions to support their online safety. ITU Member States have also indicated that there is significant support for enhanced knowledge sharing and coordinated efforts to secure the safety of greater numbers of children online[9].

Children and young people are navigating an increasingly complex digital landscape and the adoption of artificial intelligence for machine learning, big data analytics, robotics, virtual and augmented reality, and the Internet of Things are set to transform children's media practices. This requires policymaking and investment for the children, parents, and communities of the future as much as for today.

---

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

8 ITU, Youth Consultation, https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx.

9 UNICEF, "Global Kids Online Comparative Report (2019)."

10 ITU, "Celebrating 10 Years of Child Online Protection", ITU News, February 6, 2018, https://news.itu.int/celebrating-10-years-child-online-protection/.

2.1 What is child online protection?

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

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

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

While no universal definition exists for child online protection, it aims to take a holistic approach to building safe, age appropriate, inclusive and participatory digital spaces for children and young people, characterised by:

- response, support and self-help in the face of threat;
- prevention of harm;
- a dynamic balance between ensuring protection and providing opportunity for children to be digital citizens;
- upholding the rights and the responsibilities of both children and society.

Moreover, due to the rapid advancements in technology and society and the borderless nature of the Internet, child online protection needs to be agile and adaptive to be effective. While these guidelines offer insight into the leading risks to children and young people online, including harmful and illegal content, harassment, cyberbullying, misuse of personal data, or grooming for sexual purposes and child sexual abuse and exploitation, new challenges will emerge with the development of technological innovations and will typically vary from region to region. However, new challenges will be best dealt with by working together as a global community, as new solutions to these challenges need to be found.

2.2 Children in the digital world

The Internet has transformed how we live. It is entirely integrated into the lives of children and young people, making it impossible to consider the digital and physical worlds separately. One third of all Internet users today are children and young people, and UNICEF estimates that 71 per cent of young people are already online.

Such connectivity has been tremendously empowering. The online world allows children and young people to overcome disadvantages and disability, and has provided new arenas for entertainment, education, participation and relationship building. Digital platforms, today, are used for a variety of activities and are often multi-media experiences.

Having access to and learning to use and navigate this technology is seen as critical to young people's development and are first used at an early age. Policy-makers must understand that

children and young people often start using platforms and services before they reach the outline minimum age, and therefore, education must start early.

Children and young people want to be involved in the conversation, and they have valuable expertise as 'digital natives' that can be shared. Policy-makers and practitioners must engage with children and young people in an on-going debate about the online environment to support their rights.

Access of Internet

In 2019, more than half of the world's population used the Internet (53.6 per cent), with an estimated 4.1 billion users. At the global level, one-in-three Internet users is a child under 18 years of age[1]. In some lower income countries, this rises to around one-in-two while in the higher income countries, the ratio is around one-in-five. According to UNICEF, worldwide, 71 per cent of young people are already online[2]. Children and young people are therefore now a substantial, permanent and persistent presence on the Internet[3]. Internet serves other social, economic or political purposes, and has become a family or consumer product or service which is integral to the way families and children and young people live their lives.

In 2017, regionally, access to the Internet of children and young people is highly linked to the level of income. Low income countries tend to have fewer child Internet users than high income countries.

Children and young people in most countries spend more time online at the weekend than on a weekday, with adolescents (15–17 year olds) spending the longest online, at between 2.5 and 5.3 hours on average, depending on the country.

Use of the Internet

Among children and young people, the most popular device for accessing the Internet is the mobile phone, followed by desktop computers and laptops. Children and young people spend on average about two hours a day online during the week and roughly double that each day of the weekend. Some feel permanently connected. But many others still do not have access to the Internet at home.

---

1 Livingstone, S., Carr, J., and Byrne, J. (2015) *One in three: The task for global internet governance in addressing children's rights*. Global Commission on Internet Governance: Paper Series. London: CIGI and Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

2 Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)," *Broadband Commission for Sustainable Development,* October 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

3 Livingstone, Carr, and Byrne, "One in Three: Internet Governance and Children's Rights."

In practice, most children and young people who use the Internet, access it through more than one device: Children and young people who connect at least weekly sometimes use up to three different devices to do so. Older children and children in richer countries generally use more devices, and boys use slightly more devices than girls in every country surveyed.

The most popular activity – for both girls and boys – is watching video clips. More than three quarters of Internet-using children and young people say that they watch videos online at least weekly, either alone or with other members of their family. Many children and young people can be considered 'active socializers' using several social media platforms such as Facebook, Twitter, TikTok or Instagram.

Children and young people also engage in politics online and making their voices heard through blogging.

The overall level of participation in online gaming varies by country roughly in line with children and young people's availability of access to the Internet, while 10 to 30 per cent of Internet-using children and young people engage in creative online activities on a weekly basis.

For educative purposes, many children and young people of all ages use the Internet for homework, or even to catch up after missing classes or seek health information online on a weekly basis. Older children seem to have a greater appetite for information than younger children.

2.3 The impact of technology on children's digital experience

The Internet and digital technology can provide opportunity and present risks to children and young people. For example, when children use social media, they benefit from many opportunities to explore, learn, communicate and develop key skills. For example, social networks are seen by children as platforms that allow them to explore personal identity in a safe environment. Having the relevant skills and knowing how to tackle issues related to privacy and reputation is important to young people.

"I know everything you post on the Internet stays forever and it can affect your life in the future", Boy, 14 years old, Chile.

However, with consultations showing that most children using social media before the minimum age of thirteen[11], and age verification services being generally weak or lacking, the risks facing children can be intensified. And while children want to learn digital skills and become digital citizens, in particular caring about their privacy, they tend to think about privacy in relation to their friends and acquaintances – "What can my friends see?" – and less so in relation to strangers and third parties. Combined with children's natural curiosity and generally lower threshold for risk, this can make them vulnerable to grooming, exploitation, bullying or other types of harmful content or contact.

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

The widespread popularity of image and video sharing via mobile apps, and particularly the use of live streaming platforms by children presents further privacy and risk-related concerns. Some children are producing sexual images of themselves, friends and siblings and sharing them online. For some, particularly older children, this can be seen as the natural exploration of sexuality and sexual identity, while for others, particularly younger children there is often coercion by an adult or other child. Whatever the case, the resulting content is in many countries illegal and may expose children to the risk of prosecution, or it may be used to further exploit the child.

Similarly, online gaming enables children to fulfil their fundamental right to play, as well as to build networks, spend time with and meet new friends, and to develop important skills. Overwhelmingly, this can be positive. However, there is increasing evidence to indicate that left unmonitored and unsupported by a responsible adult, online gaming platforms can also pose risks to children, from gaming disorders, financial risks, collection and monetization of children's personal data, to cyberbullying, hate speech, violence, and exposure to inappropriate conduct or content[12], and grooming using real, computer generated or even virtual reality images and videos depicting and normalizing the sexual abuse and exploitation of children.

Furthermore, developments in technology have led to the emergence of the Internet of Things, where an increasing number and range of devices are able to connect, communicate and network over Internet. This includes toys, baby monitors and devices powered by artificial intelligence that may present risks in terms of privacy and unwanted contact.

2.4 Key threats to children online

Adults and children are exposed to a range of risks and dangers online. Nonetheless, children are a much more vulnerable population. Some children are also more vulnerable than other groups of children, for instance children with disabilities[13] or children on the move. Policy-makers need to guarantee that all children can develop and be educated in a safe digital environment. The idea that children are vulnerable and should be protected from all forms of exploitation is outlined in the UN Convention on the Rights of the Child.

Several areas in the digital environment offer great opportunities for children but may at the same time compound risks that might harm children profoundly and undermine their well-being. There are concerns, for adults and children alike, that for example the Internet can be used to invade personal privacy, peddle disinformation, or worse, allow access to pornography.

It is crucial here to distinguish between risks and harms for children. Not every activity that may bear elements of risk is dangerous and not all risks become necessarily harmful for children, for instance, Sexting, which is a way young people might explore sexuality and relationships, and which is not necessarily harmful.

12 UNICEF, "Global Kids Online Comparative Report (2019)." (UNICEF, 2019)

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

Figure 2: Classification of online threats to children[14]

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

Source: EU Kids Online (Livingstone, Haddon, Görzig, and Ólafsson (2011)

The advent of the digital age has presented new challenges for child protection. Children must be empowered to navigate the online world safely and reap its many rewards.

Policy-makers must ensure that the relevant legislation, safeguards and tools are in place to allow children to develop and learn safely. It is critical that children are equipped with the necessary skills to identify threats, and fully understand the implications and nuances of their behaviour online.

Whilst online, children can encounter a multitude of threats from organisations, adults, and their peers.

Content and manipulation

- Exposure to inappropriate or even criminal content can lead children to extremes such as self-harm, destructive, and violent behaviours. Exposure to such content can equally lead to radicalisation or subscribing to racist or discriminatory ideas. It is recognised that many children do not abide by the age limitations placed on websites.
- Exposure to inaccurate or incomplete information limits children's understanding of the world around them. The trend of customising content based on user behaviour can lead to 'filter bubbles', restricting children from developing and reaching a broad range of content.
- Exposure to content that is algorithmically filtered with the intention to manipulate can greatly influence a child's development, opinions, values, and habits. Isolating children in 'echo chambers' or 'filter bubbles' prevent them from accessing a wide variety of opinions and ideas.

[14] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/.

Contact from adults or peers

Children can encounter a broad range of contact threats from their peers or adults.

- Online bullying can spread more widely, with a greater degree of speed, than offline. It can happen any time of the day or night, thus invading previously 'safe spaces', and can be anonymous.
- Children who are victimized offline are likely to be victimized online. This places children with disabilities at higher risk online, as research shows that children with disabilities are more likely to experience abuse of any kind, and specifically are more likely to experience sexual victimization. Victimization can include bullying, harassment, exclusion, and discrimination based on a child's actual or perceived disability, or on aspects related to their disability such as the way that they behave or speak, or equipment or services they use.
- Defamation and damage to reputation: images and videos can be altered and shared to billions of people. Ill-judged comments can be available for decades, free for anyone to view.
- Children can be targeted, groomed and abused through the Internet by an offender either locally or on the other side of the world, often claiming to be someone they are not. This can take several forms, including radicalisation or being coerced into sending sexually explicit content of themselves.
- Being pressured, duped or coerced into making purchases with or without the bill payer's permission.
- Unwanted advertising raises issues of consent and the selling of data.

Conduct of the child, potentially leading to consequences

- Online bullying can be particularly upsetting and damaging because it can spread more widely, with a greater degree of publicity, and content circulated electronically can resurface at any time, which can make it harder for the victim of the bullying to get closure over the incident; it can contain damaging visual images or hurtful words; the content is available 24 hours a day; bullying by electronic means can happen 24/7 so it can invade the victim's privacy even in otherwise 'safe' places such as their home; and personal information can be manipulated, visual images altered and these then passed on to others. Moreover, it can be carried out anonymously. Disclosure of personal information leading to the risk of physical harm, including real-life encounters with online acquaintances, with the possibility of physical and/or sexual abuse.
- Infringement of their own or the rights of others through plagiarism and uploading of content without permission, including the taking and uploading of inappropriate photos without permission.
- Infringement of other people's copyright e.g., by downloading music, films or TV programmes that ought to be paid for as this can be harmful for the victim of the theft.
- Compulsive and excessive use of the Internet and/or online gaming, to the detriment of social and/or outdoor activities important for health, confidence building, social development and general well-being.
- Attempt to harm, harass or bully someone else, including pretending to be someone else, often another child.
- An increasingly common behaviour by teenagers is 'sexting' (sharing of sexualized images or text via mobile phones). These images and text are often shared between partners in a relationship or with potential partners, but sometimes end up being shared with much wider audiences. It is thought unlikely that young teenagers have an adequate understanding of the implications of these behaviours and the potential risks they entail.

2.5 Key harms for children online

The previous section refers to the threats that children can encounter online. This section highlights the harms that can occur from those threats.

Harms

According to UNICEF studies on Internet use, the following categories are considered risks and harms:

- Self-abuse and self-harm:
  - suicidal content
  - discrimination
- Exposure to unsuitable materials:
  - exposure to extremist/violent/gory content
  - embedded marketing
  - online gambling
- About 20 per cent of children surveyed on the issue said they had seen, in the past year, websites or online discussions about people physically harming or hurting themselves.
- Radicalisation:
  - ideological persuasion
  - hate speech
- Children were more likely to report being upset by hate speech or sexual content online, being treated in a hurtful way online or offline, or by meeting someone face to face that they had first got to know online.
- Sexual abuse and exploitation:
  - self-generated content
  - Sexual grooming
  - child sexual abuse material (CSAM)
  - trafficking
  - sexual exploitation of children in travel and tourism

A 2017 study of children in Denmark, Hungary, and the United Kingdom found that 6 per cent of children had explicit pictures of them shared without their permission.

In 2019, the Internet Watch Foundation (IWF) identified more than 132,000 webpages confirmed to contain the images and videos of child sexual abuse. Each webpage could contain anything from one to thousands of images of this abuse.

The risks related to online violence, such as the dissemination of nude photos without consent and sexual cyber-bullying, are marked by unequal gender dynamics, with girls usually being more affected by gendered pressures towards sexual behaviour, experiencing consequences that are more negative and causing harm.

- Violation and misuse of personal data:

  - hacking
  - fraud and theft

  Many people are familiar with scams and hacking, but invasion of privacy regarding a child's online activities is seen as another violation. Adults often undermine the young by scrutinizing their mobile phones and surveying their activities online, for example, reports from children in Brazil show that both boys and girls, from different age ranges, perceive parents as more controlling of girls' use of the Internet. Attempts to explain this often suggest that girls may be in some cases more vulnerable due to societal structures within which they live, in particular with regard to their safety, in a context where the boundary between online and offline interaction becomes increasingly blurred.

- Cyberbullying, stalking and harassment: Hostile and violent peer activity

  Chat rooms and social network sites can open the door to violence and bullying, as anonymous users, including young people, engage in aggressive or abusive communication. Across seven countries in Europe – Belgium, Denmark, Ireland, Italy, Portugal, Romania, and the United Kingdom – Livingstone, Mascheroni, Ólafsson, and Haddon[1] found that on average, in 2010, 8 per cent of children were cyberbullied, while 12 per cent of children were victims of cyberbullying in 2014.

It is essential to point out that vulnerable children are often at a higher risk of cyberbullying victimization.

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

In focus: Enhancing inequalities

In 2017, around 60 per cent of children were not online in the Africa region, compared to only 4 per cent in Europe. Male Internet users outnumber female users in every world region, and Internet use by girls is often monitored and restricted. With the expansion of broadband to the unconnected parts of the world this inequality will significantly increase[15].

Children who rely on mobile phones rather than computers may only get a second-best online experience. Children who speak minority languages often cannot find relevant content online, and children from rural areas are more likely to experience theft of passwords or money.

[15] Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)."

Research shows, that many adolescents worldwide must navigate significant barriers to their online participation. For many, access challenges – poor connectivity, prohibitive costs of data and devices, and a lack of appropriate equipment – remain key barriers.

With the expansion of affordable broadband to the developing world, there is an urgent need to put in place measures to minimize the risks and threats to these children, while also allowing them to capitalize on all the benefits the digital world.

In Focus: Child Sexual Abuse Material (CSAM)

The scale of the problem

The Internet has transformed the scale and nature of the production, distribution and availability of CSAM. In 2018, technology companies based in the United States of America reported over 45 million online images and videos suspected to show children being sexually abused from around the world. This is a global industry and the scale and severity of the abuse is increasing despite efforts to stop it.

Historically, in an offline world, finding CSAM required offenders to take considerable risks, at significant expense, to access the material. With the Internet, offenders can now access this material relatively easily and engage in increasingly risky behaviour. Cameras are smaller, increasingly integrated into every aspect of our lives, making the process of producing CSAM and acquiring content from non-contact abuse easier than it has ever been.

It is impossible to determine the precise size or shape of this clandestine and illegal enterprise. However, it is clear that the number of illegal images now in circulation can be counted in the millions. Almost all the children involved in the images have had their image duplicated. In 2018, the IWF tracked how often images surfaced of a child who was known to have been rescued in 2013. Over the three months, IWF analysts tracked the images 347 times – 5 times every working day.

The current landscape

Every time an image of a child being abused appears and reappears online, or is downloaded by an offender, that child is being re-abused. Victims are forced to live with the longevity and circulation of these images for the rest of their lives.

As soon as material depicting, or a webpage hosting, child sexual abuse is discovered, it is important to remove or block the content as quickly as possible. The global nature of the Internet makes this difficult: offenders can produce material in one country and host it in another for consumers in a third. It is almost impossible for national warrants or notices to be enacted without sophisticated international cooperation.

The pace of innovation within the digital world means that the offender landscape is constantly shifting. Key threats that have recently emerged include:

- The rise of encryption inadvertently allows offenders to operate and share material with hidden channels, whilst equally making detection and law enforcement more challenging.
- Forums dedicated to the grooming of children are growing in shielded corners of the Internet, normalizing and encouraging this behaviour, often requiring 'new content' to join.
- The rapid expansion of the Internet is enabling users to go online in areas that yet to develop/implement a comprehensive safeguard strategy or the relevant infrastructure.

- Children are using devices unsupervised at younger ages, and sexual behaviour online is being normalized. The number of self-generated images of abuse is rising each year.

In Focus: Self-generated content

Children and adolescents may take compromising pictures or videos of themselves. While this conduct in itself is not necessarily illegal and may take place as part of normal, healthy sexual development, there are risks that any such content can be circulated online or offline to harm children or be used as a basis to extort favours. Although some children may be pressured or coerced to share sexual images, others, (in particular adolescents) may willingly produce sexual content. This does not mean that they consent to or are responsible for the exploitative or abusive use and/or distribution of these images.

Sexting has been defined as the "self-production of sexual images",[16] or as the "exchange of sexual messages or images" and "the creating, sharing and forwarding of sexually suggestive nude or nearly nude images through mobile phones and/or the Internet"[17]. Sexting is a form of self-generated sexually explicit content,[18] and the practice is "remarkably varied in terms of context, meaning, and intention"[19].

While sexting is possibly the most common form of self-generated sexually explicit content involving children, and is often done by and among consenting adolescents who derive pleasure from the experience, there are also many forms of unwanted sexting. This refers to the non-consensual aspects of the activity, such as sharing or receiving unwanted sexually explicit photos, videos, or messages, for instance by known or unknown persons trying to make contact, put pressure on, or groom the child. Sexting can also be a form of sexual bullying, where a child is pressured to send a picture to a boyfriend/girlfriend/peer who then distributes it to a peer network without their consent.

In Focus: Cyberbullying

While bullying as a phenomenon far pre-dates the Internet, the added scale, scope and continuity of bullying committed online can exacerbate further what is already an upsetting and often harmful experience for its victims. Cyberbullying is defined as wilful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices. It often takes place in parallel to offline bullying taking place at school or elsewhere, it can have additional racist, religious or sexist dimensions, and it can constitute an extension of the harm caused offline, such as through account hacking, the spread photos and videos online and the 24/7 nature of the hurtful messages and availability of content. Generally, a social issue rather than criminal in nature, policies to address cyber-bullying require a holistic approach that involves schools, families and crucially children themselves.

In Focus: Online grooming and sextortion

---

16 Karen Cooper et al., "Adolescents and Self-Taken Sexual Images: A Review of the Literature," *Computers in Human Behaviour* 55 (February 2016): 706–16, https://doi.org/10.1016/j.chb.2015.10.003.

17 Jessica Ringrose et al., "A Qualitative Study of Children, Young People and 'Sexting': A Report Prepared for the NSPCC" (London, UK: National Society for the Prevention of Cruelty to Children, 2012), http://doi.wiley.com/10.1046/j.1365-2206.1997.00037.x.

18 UNODC, "Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children" (Vienna: UN, 2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.[3] UNODC, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, p.22.

19 Cooper et al., "Adolescents and Self-Taken Sexual Images."

With the rapid advances in technology and increased access to the Internet and digital communications experienced in recent years, a heightened risk of online criminal acts targeting children has inevitably followed. Among these emerging forms of online child sexual exploitation are online grooming and sextortion of children. Online grooming broadly refers to the process of an adult befriending and influencing a child (under the age of 18 years), through the use of the Internet or other digital technologies, to facilitate contact or non-contact sexual interaction with that child. Through the grooming process, an offender tries to gain the child's compliance to maintain secrecy and to avoid detection and punishment[20]. It is important to recognise that there are also instances of peer-on-peer abuse.

INTERPOL reports that the Internet facilitates grooming by virtue of having a large number of easily accessible potential targets and making it possible for groomers to present themselves in a way that is attractive to the child. Online child sex offenders use manipulation, coercion, and seduction to lower inhibitions and entice children to engage in sexual activity. The groomer undertakes a deliberate process of identifying a vulnerable potential victim, intelligence gathering on the child's family support, and uses pressure or shame/fear to sexually abuse a child. Groomers may use adult pornography and child abuse or exploitation material to disinhibit their potential targets, presenting child sexual activity as natural and normal. The Internet has changed the way in which people interact and has redefined the concept of 'friend'. A groomer can establish a friendship with a child online very easily and quickly, which forces a reassessment of the traditional 'stranger danger' education messages.

Online grooming was first formally recognized in an international legal instrument in 2007 by the **Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse** (Lanzarote Convention). Article 23 criminalizes the "solicitation of children for sexual purposes," which requires that there is an intentional proposal to meet the child for the purpose of committing a sexual offence which is followed by "material acts leading to such a meeting." In many grooming cases, children are sexually abused and exploited online – the 'meeting' required by the Lanzarote Convention and many existing national laws is entirely virtual – but is, nonetheless, equally harmful to the child as a physical meeting. It is crucial that criminalization of grooming extends "to cases when the sexual abuse is not the result of a meeting in person but is committed online"[21].

Sextortion[22] can occur as a feature of online grooming or as a standalone offence. While sextortion can occur without the online grooming process, in some cases online grooming may lead to sextortion[23]. Sextortion may occur in the context of online grooming as a groomer manipulates and exerts influence over the child during the grooming process through threats,

---

20 International Centre for Missing & Exploited Children, "Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review," 1st Edition (International Centre for Missing & Exploited Children, 2017), https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.

21 Lanzarote Committee, Committee of the Parties to the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, *Solicitation of children for sexual purposes through information and communication technologies (grooming), Opinion on Article 23 of the Lanzarote Convention and its explanatory note*, Jun. 17, 2015, *at https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html* (last visited Nov. 6, 2019).

22 National Center for Missing and Exploited Children (NCMEC), *Sextortion*, *at* http://www.missingkids.com/theissues/onlineexploitation/sextortion (last visited Nov. 6, 2019).

23 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27-28, *at* http://luxembourgguidelines.org/english-version.

intimidation, and coercion to send sexual images of themselves (self-generated content)[24]. If the victim fails to provide the requested sexual favours, additional intimate images, money, or other benefits, his or her images may be posted online for the purpose of causing humiliation or distress or coercing the child into generating additional sexually explicit material[25].

Sextortion has been referred to as "virtual sexual assault" because of the similar emotional and psychological effects on victims[26]. In some instances, the abuse is so traumatizing that victims have attempted to self-harm or commit suicide as a means of escaping the abuse.

Europol noted that collecting information to assess the scope of sextortion affecting children is challenging and may be heavily underreported[27]. Additionally, the lack of common terminology and definitions for online grooming and sextortion are barriers to the collection of accurate data and an understanding of the true scope of the issues globally.

2.6 Children with vulnerabilities

Children and young people can be vulnerable for a variety of different reasons. Research carried out in 2019 stated that "vulnerable children's digital lives seldom receive the same nuanced and sensitive attention that "real life" adversity tends to attract". Furthermore, the report goes on to say that "at best they [children and young people] receive the same generic online safety advice as all other children and young people, while specialist intervention is required".

Three examples of specific vulnerabilities are: migrant children, children with autism spectrum disorder and children with disabilities), but of course there are many others.

Migrant children

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

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

[24] Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27-28, *at* http://luxembourgguidelines.org/english-version.

[25] Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27-28, *at* http://luxembourgguidelines.org/english-version.

[26] Benjamin Wittes et al., "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault" (Brookings Institution, May 11, 2016), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.

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

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

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

Children with Autism Spectrum Disorder (ASD)

The autism spectrum summarises two core domains in DSM-5 behaviour diagnostic process:

- restricted and repetitive behaviour ("the need for sameness");
- difficulty with social and communicative behaviours;
- frequent co-occurrence with intellectual disability, language issues and similar.

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

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

Children with disabilities

Children with disabilities face risks online in many of the same ways as children without disabilities, but they may also face specific risks related to their disabilities. Children with disabilities often face exclusion, stigmatization, and barriers (physical, economic, societal and attitudinal) to participating in their communities. These experiences can contribute to a child with a disability seeking out social interactions and friendships in online spaces, which can be positive, build self-esteem and create support networks. However, it can also place them at greater risk for incidents of grooming, online solicitation, and/or sexual harassment – research shows that children experiencing difficulties offline and those affected by psychosocial difficulties are at heightened risk for such incidents[28].

Overall, children who are victimized offline are likely to be victimized online. This places children with disabilities at higher risk online, yet they have a greater need to be online. Research shows that children with disabilities are more likely to experience abuse of any kind[29], and specifically are more likely to experience sexual victimization[30]. Victimization can include bullying, harassment, exclusion, and discrimination based on a child's actual or perceived

[28] Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content," *Berkman Center for Internet & Society, Harvard University*, December 2008, 87, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.'

[29] UNICEF, "State of the World's Children Report: Children with Disabilities," 2013, https://www.unicef.org/publications/files/SOWC2013_Exec_Summary_ENG_Lo_Res_24_Apr_2013.pdf.

[30] Katrin Mueller-Johnson, Manuel P. Eisner, and Ingrid Obsuth, "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors," *Journal of Interpersonal Violence* 29, no. 17 (November 2014): 3180–3206, https://doi.org/10.1177/0886260514534529.

disability, or on aspects related to their disability such as the way that they behave or speak, equipment or services they use.

Perpetrators of grooming, online solicitation, and/or sexual harassment towards children with disabilities can include not only offenders who target children, but also those who target children with disabilities. Such offenders may include 'devotees' – nondisabled persons sexually attracted to persons with disabilities (most commonly amputees and persons using mobility aids), some of whom even pretend to be disabled themselves[31]. Actions by such people may include downloading photos and videos of children with disabilities (that are innocuous in nature), and/or sharing them through dedicated forums or social media accounts. Reporting tools on forums and social media often do not have a targeted or appropriate pathway to deal with such actions.

There are concerns that 'sharenting' (parents sharing information and photos of their children online) can violate a child's privacy, lead to bullying, cause embarrassment, or have negative consequences later in life[32]. Parents of children with disabilities may share such information in search of support or advice, placing children with disabilities at higher risk for adverse outcomes.

Some children with disabilities may face difficulties in using, or even exclusion from online environments due to inaccessible design (e.g. apps that don't allow text size to be increased), denial of requested accommodations (e.g. screen reader software or adaptive computer controls), or the need for appropriate support (e.g. coaching in how to use equipment, one on one support to navigating social interactions[33]).

In relation to the contract risk or signing the terms and conditions, children with disabilities are at higher risk of accepting legal terms that sometimes not even adults can understand.

2.7 Children's perceptions of online risks

Worldwide exposure to violence, access to inappropriate content, goods and services; concerns about excessive use; issues of data protection and privacy are those risks highlighted by children[34].

Adolescents report a range of concerns regarding their engagement with digital technologies. These include commonly discussed online safety concerns such as fears of interacting with strangers online, accessing inappropriate content, or being exposed to malware or viruses – while others relate to the reliability of their access to technology; parental intrusion into their 'private' lives online; and their digital literacy skills[35].

---

31 Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder," *Sexual and Disability* 15, no. 4 (1997): 18, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.

32 UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy," Innocenti Discussion Paper 2017-03 (UNICEF, Office of Research-Innocenti), accessed January 16, 2020, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.

33 For guidelines on these rights, see the Convention on the Rights of Persons with Disabilities Article 9 on Accessibility and Article 21 on Freedom of expression and opinion, and access to information.

34 Amanda Third et al., "Children's Rights in the Digital Age" (Melbourne: oung and Well Cooperative Research Centre, September 2014), http://www.uws.edu.au/__data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf.

35 Amanda Third et al., "Young and Online: Children's Perspectives on Life in the Digital Age," The State of the World's Children 2017 Companion Report (Sydney: Western Sydney University, 2017). The report summarized the views of 490 children aged 10–18, from 26 different countries speaking 24 official languages.

EU Kids Online research shows that pornography and violent content top children's online concerns in Europe. Overall, boys appear more bothered by violence, while girls are more concerned with contact-related risks[36]. Concern about risks is higher among children from 'high use, high risk' countries.

In Latin America, child consultations have shown, that a loss of privacy, violence and harassment are the main concerns[37]. Children report being contacted by people they don't know – this is especially the case when playing games online. In such situations, the main strategy seems to not engage and/or to block the person. Girls are confronted with harassment in social media from an early age. They manage to navigate these forms of violence on their own, blocking users, and changing privacy settings. Harassment comes from users that sometimes don't speak Spanish, but manage to send them images, request friendship, and comment on their posts. Some boys also report having received such requests.

In many parts of the world, children have a good understanding of some of the risks they face online[38]. Research has shown that the majority of children are able to distinguish cyberbullying from joking or teasing online, recognising that cyberbullying has a public dimension and is designed to harm[39].

[36] Livingstone, S. (2014) *EU Kids Online: Findings, methods, recommendations*. LSE, London: EU Kids Online, https://lsedesignunit.com/EUKidsOnline/.
[37] Contectados al Sur network, "Hablatam."
[38] Since 2016, ITU undertakes consultations within COP with children and adult stakeholders on relevant issues such as cyberbullying, digital literacy and children's activities online.
[39] UNICEF, "Global Kids Online Comparative Report (2019)."

3. Preparing for a national child online protection strategy

In developing a national child online protection strategy to promote online safety for children and young people, national governments and the policy-making institutions need to identify best practice and engage with key stakeholders.

The following sections highlight the typical actors and stakeholders together with an outline of their potential role and responsibilities with regards to protecting children online.

3.1 Actors and stakeholders

Policy-makers may identify suitable individuals, groups and organisations representing each of these actors and stakeholders within their jurisdiction. Appreciating each of their current, planned and potential activities is important in any national coordination and orchestration of child online protection strategies.

Children and young people

Across the world children and young people have shown that they can adapt to and use new technologies with great ease. The Internet is becoming increasingly important within schools and as an arena where children can work, play, and communicate.

According to the latest report of ChildFund Alliance, only 18.1 per cent of children interviewed think that the people who govern act to protect them. It is important that policy-makers engage with children in this regard, recognising their right to be heard (Art. 12 CRC).

To be able to protect children, policy-makers should standardize the definition of a child in all legal documents. A child should be defined as anyone under the age of 18. This is consistent with Article 1 of the UN Convention on the Rights of the Child (UNCRC), which states that "a child means every human being below the age of 18 years". Companies should not be allowed to treat as an adult, anyone who is under 18 but legally old enough to consent to data processing. This narrow definition is not justified by any evidence on childhood development milestones. It undermines the rights and threatens the safety of children.

Whilst many children may appear confident in using technology, many feel unsafe[40] online and have several concerns[41] regarding the Internet.

Children's and young people's lack of experience of the wider world can render them vulnerable to a range of risks. They have a right to expect help and protection. It is also important to remember that not all children and young people will experience the Internet or the new technologies in the same way. Some children with special needs caused by physical or other disabilities may be particularly vulnerable in an online environment and will need extra support.

Surveys have repeatedly shown that what adults think children and young people are doing online and what is actually happening can be very different. Half of all children surveyed said

[40] ChildFund Alliance, "VIOLENCE AGAINST CHILDREN AS EXPLAINED BY CHILDREN," Save Voices Big Dreams, 2019, https://childfundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee81cb216/SVBD-THE_REPORT-digital.pdf.

[41] Council of Europe, "It's Our World: Children's Views on How to Protect Their Rights in the Digital World," Report on child consultations (Council of Europe, Children's Right Division, October 2017), https://rm.coe.int/it-s-our-world-children-s-views-on-how-to-protect-their-rights-in-the-/1680765dff.

that in their country adults do not listen to their opinion on issues that matter to them[42]. For this reason, it is important to ensure, in whatever arrangements are made at the national level to develop policy in this area, that appropriate mechanisms are found to enable all children's and young people's voices to be heard and that their concrete experiences of using the technology are taken into account.

Parents, guardians, and educators

Parents, guardians and educators spend the most time with children. They should be educated in digital literacy to understand the online environment and be able to protect children and teach them how to protect themselves.

Educational institutions have a particular responsibility to teach childrenabout how to stay safer online, whether they are using the Internet in school, at home or anywhere else, and policy-makers should include in national curricula digital literacy from a very early age (3 to 18 years old). This would allow children to be able to protect themselves, know their rights and, therefore, use the Internet as an enabler of knowledge[43] .

Policy-makers are reminded that parents and guardians will almost always be the first, last and best line of defence and support for their own children. Yet when it comes to the Internet, they might feel a little lost. Again, schools can act as an important channel for reaching out to parents and guardians, to make them aware both of the risks and the many positive possibilities which the new technologies present. However, schools should not be the only route used to reach out to parents and guardians. It is important to use many different channels to maximize the possibility of reaching out to the greatest possible number of parents and guardians. Industry has a significant role here in supporting their users or customers. Parents and guardians may choose to manage their child's online activity and access, talk with the child about the correct behaviour and usage of technologies, understand what the child is doing online so the family conversation integrates the online and offline experiences as one.

Parents and guardians also need to be a good example to their children on how to use their devices and behave in an appropriate way on the Internet.

Policy-makers should be reminded that parents and carers should be consulted to obtain their views, experiences and understanding of protecting their children online.

Finally, policy-makers together with other public institutions can develop public awareness campaigns, including for parents, caregivers and educators. The public libraries, health centres, even shopping malls and other major retail centres can all provide accessible venues for the presentation of e-safety and digital skills information. When implementing this task, governments should ensure there is neutrality in the advice given, free from any private interest, and cover a wide variety of issues within the digital space.

Industry

Industry is one of the key stakeholders in the ecosystem as the sector possesses the technological knowledge that policy-makers need to address and understand in order to develop the legal

[42] ChildFund Alliance, "Violence against children as explained by children."

[43] UNICEF, "Policy Guide on Children and Digital Connectivity" (Policy Lab, Data, Research and Policy, United Nations Children's Fund, June 2018), https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf.

framework. Thus, it is of the essence that policy-makers engage industry in the process of elaborating the child online protection laws.

Also, it is important to encourage industry to incorporate in their business a safety by design approach when developing new technology. Clearly, companies that are developing or providing new technology products and services should help their users to understand how they work and how to use them safely and appropriately.

Industry also has a major responsibility to help promote awareness of the online and safety agenda, particularly to children and their parents or guardians, but also to the wider community. By engaging in this way, industry stakeholders will learn more about other stakeholder concerns and the risks and harms to which the end users are being exposed. With that knowledge, the Industry could correct existing products and services, and identify hazards in development.

Recent advances in artificial intelligence are paving the way for industry to build in much more robust checks and balances to identify the user and to provide children with a conducive environment for positive online behaviour. These advances could also pose new risks to children.

In some countries the Internet is governed by a framework of self-regulation or co-regulation. However, some countries are considering, or have implemented, legal and regulatory frameworks, including obligations for companies to detect, block and/or remove harm against children from platforms or services, as well as to provide clear reporting routes and access to support.

The research community and non-governmental organizations

Within universities and the research community, there is very likely to be a range of academics and scholars who have a professional interest in and a very detailed knowledge of the social and technical impact of the Internet. They are a very valuable resource in terms of helping national governments and policy-makers to develop strategies, which are based on hard facts and good evidence. They can also act as an intellectual counterweight to business interests that can sometimes be too short term and commercial.

Similarly, within the non-governmental organization (NGO) community there is a range of expertise and information that can be an invaluable resource in reaching out or providing services to children, parents, carers and educators to help promote the online safety agenda and more generally, defend the public interest.

Law enforcement

It is a sad fact that as wonderful as technology is, it has also attracted the attention of criminal and anti-social elements. The Internet has greatly increased the circulation of CSAM and other online harms. Sexual predators have used the Internet to make initial contact with children luring them into very harmful forms of contact, online and offline. Bullying and other forms of harassment can do great harm to children's lives and the Internet has provided a new way for that to happen.

For these reasons, it is essential that the law enforcement community becomes fully engaged with any overall strategy to help make the Internet safer for children and young people. Law enforcement officers need to be appropriately trained to conduct investigations into Internet related crimes against children and young people. They need the right level of technical

knowledge and access to forensic facilities to enable them to extract and interpret data obtained from computers or the Internet in the least amount of time.

In addition, it is very important that law enforcement establishes clear mechanisms to enable children and young people, or any member of the public, to report any incidents or concerns they might have about a child's or a young person's online safety. Many countries, for example, have established hotlines to facilitate reports of CSAM and similar dedicated mechanisms exist to facilitate reports of other kinds of issues, for example bullying. Policy-makers should work with the International Association of Internet Hotlines (INHOPE), supporting them in assessing and processing CSAM reports and benefitting from the INHOPE assistance to organisations around the world in setting up a hotline where there is none. Policy-makers should ensure there are open communication channels between law enforcement and other stakeholders. Law enforcement is the primary source for CSAM seized within national borders. A process should be put in place to examine this material in order to establish whether local victims can be identified. Where this is not possible the material should be passed onto INTERPOL for inclusion in the ICSE Database. As it is a global threat, policy-makers need to ensure international cooperation between law enforcement agencies around the world. This would reduce the time of formal processes and allow the agents to have a quicker response.

Social services

Where children or young people have been harmed or abused online, for example by having an inappropriate or illegal picture posted of them, they are likely to need specialized and long-term support or counselling. There may also be a need for wrap around services and restorative practices for offenders, particularly young offenders who also may have been victims of online or offline abuse. Professionals working within social services will need to be appropriately trained to be able to provide this kind of support. The support should be given through online and offline channels.

Health care services

The health care service needed after any case of violence against a child should be covered by the basic plan of health care at national level. The health care institutions should carry out mandatory reporting of abuse. Health care professionals should be suitably equipped and knowledgeable in order to be able to support children in this regard. Health care services should extend to include support for children's mental health and wellbeing.

Government Ministries

Child Online Protection policy will fall within the jurisdiction of a number of Government Ministries and is important to engage all these for any successful national strategy and action plan. These may include:

- Internal Affairs
- Health
- Education
- Justice
- Digital / Information
- Regulators

Regulators are best positioned to contribute to the role of controller and accountant in collaboration with the government institutions. This might include media and data protection regulators.

Broadband, mobile, and Wifi network operators

Operators may detect, block, and report illegal content within their network and provide family friendly tools, services and configurations for the use of parents in choosing how to manage their children's access. It is important for providers to equally ensure that civil liberties and privacy are respected.

Children's Rights

Independent human rights institutions for children can play a crucial role in ensuring children's protection online. Although their mandates vary, such institutions often have functions to:

- monitor the impact of law, policy and practice on the protection of children's rights;
- promote the implementation of international human rights standards at the national level;
- investigate violations of children's rights;
- provide expertise on children's rights to the courts;
- ensure that the views of children are heard on matters concerning their human rights, including the development of relevant law and policy;
- promote public understanding and awareness of children's rights; and
- undertake human rights education and training initiatives.

It is important to include direct consultation with children as is their right under article 12 of the UNCRC. The advisory, investigatory, awareness-raising and educational functions of independent human rights institutions for children are all relevant for preventing and responding to the harm that children can experience online. Such institutions should therefore be at the heart of developing a comprehensive, rights-based approach to strengthening the legal, regulatory and policy frameworks governing child online protection, including direct consultation with children, as is their right under art. 12 UNCRC.

In recent times, there have also been examples of jurisdictions introducing or considering the introduction of state agencies with a specific mandate to support the rights of the child online, including their protection from violence or harm. Where such agencies exist, they should also be closely associated with efforts to strengthen the response to child online protection at the national level.

3.2 Existing responses for child online protection

Several initiatives have been developed in order to act at national and international levels in the face of the increasing importance of ICTs in the lives of children worldwide and the inherent risks for the youngest in our societies.

National models

At the national level, several legislations should be highlighted as covering important aspects of a comprehensive framework on Child Online Protection. These include, but are not limited to:

- Audiovisual Media Services Directive (AVMSD) (reviewed 2018, EU)
- General Data Protection Regulation (GDPR) (2018, EU)

There have been innovative developments in the regulatory and institutional response of member States to threats to children's safety and wellbeing online. There is no single way to respond to CSAM, cyberbullying and other harms children encounter online, but it is notable that there have been new approaches tried in the last few years:

The Age-Appropriate Design Code (2019, UK)

In early 2019, the Information Commissioners Office published proposals for its 'age-appropriate design code' to further child protection online. The proposed code centred the best interests of the child, as laid out in the UNCRC, and set out several expectations for industry. These include robust age-verification measures, location services to be off by default for children, for industry to collect and retain only the minimum amount of personal data of children, for products to be safe by design and for explanations to be age appropriate and accessible.

The Harmful Digital Communications Act (reviewed 2017, New Zealand)

The 2015 legislation made cyber abuse a specific crime and focusses on a broad range harms, from cyber-bullying to revenge porn. It aims to deter, prevent and lessen digital harmful communication, making it illegal to post a digital communication with the intention of causing serious emotional distress to someone else, and sets out a series of 10 communication principles. It empowers users to complain to an independent organisation if these principles are broken or apply for court orders against the author or host of the communication if the issue is not resolved.

The eSafety Commissioner (2015, Australia)

The eSafety Commissioner is the world's first government agency dedicated specifically to online safety. Established in 2015, eSafety has a legislated role to lead, coordinate, educate and advise on online safety issues to ensure all Australians have safe, positive and empowering experiences online. eSafety administers investigatory schemes that focus on a range of harms including serious cyberbullying of children, image-based abuse, and prohibited content. It has the power to investigate and take action to address complaints or reports involving these types of harms – including, in some cases, the power to issue notices to individuals and to online services for the removal of material. Alongside its investigatory powers, eSafety adopts a whole of community approach, which draws upon social, cultural and technological initiatives and interventions. Its prevention, protection and proactive efforts provide a comprehensive approach to online safety.

International models

At the international and transnational level recommendations and standards have been issued by different stakeholders. These guidelines build upon the work of the following efforts:

Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment[44].

[44] Council of Europe (2020), The Digital Environment,,https://www.coe.int/en/web/children/the-digital-environment. The Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment is the first such set of standards adopted by an intergovernmental body (CM/Rec, 2018).

The guidelines are addressed to all member states of the Council of Europe, for the purpose of assisting member states and other relevant stakeholders in their efforts to adopt a comprehensive, strategic approach in maximising the full range of children's rights in the digital environment. Among the many topics covered are the protection of persona data, provision of child-friendly content adapted to their evolving capacities, helplines and hotlines, vulnerability and resilience, as well as the role and responsibilities of business enterprises. In addition, the guidelines call upon states to engage with children, including in decision-making processes, to ensure that national policies adequately address developments in the digital environment. The guidelines are currently available in 19 languages. They will be accompanied by a child friendly version of the document, as well as a Handbook for policy-makers, which will provide concrete measures on how to implement the guidelines.

Council of Europe – Lanzarote Convention

Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), which requires States to offer a holistic response to sexual violence against children, through the "4ps approach": Prevention, Protection, Prosecution and Promotion of national and international cooperation. The Convention's operation in relation to the digital environment has been clarified by the Committee of the Parties to the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the "Lanzarote Committee"), through the adoption of a number of documents. These are: an Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children (6 June 2019); an Interpretative Opinion on the applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of ICTs (12 May 2017); a Declaration on web addresses advertising child sexual abuse material or images or any other offences established in accordance with the Lanzarote Convention (16 June 2016); and an Opinion on Article 23 of the Lanzarote Convention – Solicitation of children for sexual purposes through information and communication technologies (Grooming). The Lanzarote Committee carries out monitoring on the implementation of the Convention: its 2nd thematic monitoring round of the Committee focuses on the protection of children against sexual exploitation and sexual abuse facilitated by ICTs: a report will be published on the monitoring round in 2020. As of 2019, there are 46 States Parties to the Convention, including Tunisia – the first non-member state to accede.

Further Council of Europe guidelines

Further Council of Europe standards and tools contribute to a collective acquis for a comprehensive framework aimed at all stakeholders. The Council of Europe's Convention on Cybercrime contains obligations for Parties to criminalise an array of offences related to child sexual abuse material: it is currently ratified by 64 States Parties. The Council of Europe focuses, inter alia, on empowering children and those around them to navigate the digital sphere safely. This is promoted through educational tools, including a fully revised Internet Literacy Handbook (2017), a Digital Citizenship Education Handbook (2019) and manuals aimed at parents (Parenting in the digital age – Parental guidance for the online protection of children from sexual exploitation and sexual abuse (2017); Digital citizenship…and your child – What every parent needs to know and do (2019). Finally, the Council of Europe has undertaken consultative research with children in relation to their rights in the digital environment - It's our world: Children's views on how to protect their rights in the digital environment (2017) and conducted some of the first consultative research focusing on children with disabilities'

experiences in the digital environment - Two clicks forward and one click back: Report on children with disabilities in the digital environment (2019).

Child Online Safety Report

Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online + Child Online Safety Universal Declaration[45].

OECD Recommendations on the Protection of Children Online (2012 / Review 2019-2020) Other national and transnational Initiatives should further be highlighted as supporting international cooperation as well as national effort to establish child online protection strategies. These are for instance:

The International Child Sexual Exploitation image database

Managed by INTERPOL, the International Child Sexual Exploitation image database (ICSE DB) is a powerful intelligence and investigative tool which allows specialized investigators to share data with colleagues across the world. Available through the INTERPOL secure global police communications system (known as I-247), the ICSE DB uses sophisticated image comparison software to make connections between victims, abusers and places. The ICSE DB enables certified users in member countries to access the database in real time – interrogate existing holdings, upload new data, triage and sort material, deconflict, conduct analysis and communicate with other experts around the world in response to queries related to child sexual exploitation investigations.

The WePROTECT Global Alliance

The WePROTECT Global Alliance (WPGA) is a global movement that brings together the influence, expertise and resources required to transform how online child sexual exploitation (OSCE) is dealt with worldwide. It is a partnership of governments, global technology companies, and civil society organisations. Its multi-stakeholder nature is unique in this field. The WePROTECT Global Alliance vision is to identify and safeguard more victims, apprehend more perpetrators, and end online child sexual exploitation.

The WeProtect Global Alliance comprises of a number of components, specifically a Model National Response and a Global Strategic Response. Further details can be found in Appendix 3.

The 2020 Child Online Safety Index

The DQ Institute 2020 Child Online Safety Index (COSI) is the world's first real-time analytic platform to help nations better monitor the status of their children's online safety.

The COSI is based on six pillars which form the COSI framework. Pillars one and two, Cyber Risks and Disciplined Digital Use, relate to wise use of digital technology. Pillars three and four, Digital Competency and Guidance and Education, are related to empowerment. The final two pillars relate to infrastructure, these are the pillars of Social Infrastructure and Connectivity.

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

3.3 Examples of responses to online harms

There are a number of examples of responses to online harms in Appendix 4. These examples span Educational responses, legislative and identification of online harms.

3.4 Benefits of a national child online protection strategy

Harmonisation of Laws

The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes is central to achieving global cybersecurity. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime, protect children online and facilitate international cooperation[46].

The development of adequate national legislation, the related cybercrime legal framework, and within this approach, harmonization at the international level is a key step towards the success of any national strategy for child online protection. This requires first and foremost the necessary substantive criminal law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and CSAM, whilst also taking care that children are not unduly criminalised. The fact that provisions exist in the criminal code that are applicable to similar acts committed in the real world does not mean that they can be applied to acts committed over the Internet as well. Therefore, a thorough analysis of current national laws is vital to identify any possible gaps. The next step would be to identify and define legislative language and reference material that can assist countries in the establishment of harmonized cybercrime laws and procedural rules. Such practical instruments can be used by countries for the elaboration of a cybersecurity legal framework and related laws. ITU has been working with Member States and relevant stakeholders in this direction and is heavily contributing to the advance the global harmonization of cybercrime laws.

Given the fast pace of technological innovation, self-regulation and co-regulation have been put forward as potential solutions to the obsolescence of existing regulation and to the lengthy legislative process. However, in order to be effective, regulators/policy-makers need define clearly certain child protection online objectives and challenges, put in place a clear review process and methodology for assessing the effectiveness of self-regulation and co-regulation, and in the event that self-regulation and co-regulation fails to address the identified challenges, initiate a formal legislative process to address those challenges. Also, successful self-regulatory measures could gradually be adopted into formal law within the legislative process to become a legal backstop and prevent a roll back or termination of adherence to certain self-regulatory initiatives.

[46] Broadband Commission for Sustainable Development (2019)

Coordination

It is likely, across the range of actor and stakeholders, that there are already a range of existing activities and actions with the objective to protect children online, but that these have occurred in isolation. Understanding these is important in appreciating existing efforts in the development of the national child online protection strategy. The strategy will coordinate and direct efforts through the orchestration of both existing and new activities.

4. Recommendations for frameworks and implementation

Governments must address all manifestations of violence against children in the digital environment. However, measures taken to protect children in the digital environment should not unduly restrict the exercise of other rights, such as the right to freedom of expression, the right to access information or the right to freedom of association. Rather than curtailing children's natural curiosity and sense of innovation for fear of encountering risks online, it is critical to tap into children's resourcefulness and enhance their resilience while exploring the potential of the digital environment.

In many instances, acts of violence against children are committed by other children. In such situations, governments should as far as possible pursue restorative approaches that repair the harm done, while preventing the criminalization of children. Governments should promote the use of ICTs in preventing and addressing violence, such as the development of technologies and resources for children to access information, block harmful material and report instances of violence when they occur[47].

To face the global child online safety situation, governments must facilitate the communication between their relevant entities and cooperate openly to eliminate harm to children online.

4.1 Framework recommendations

4.1.1 Legal Framework

Governments should review and, where necessary, update its legal framework to support the full realization of the rights of the child in the digital environment. A comprehensive legal framework should address preventive measures; prohibition of all forms of violence against children in the digital environment; provision of effective remedies, recovery and reintegration to address violations of children's rights; the establishment of child-sensitive counselling, reporting and complaint mechanisms; and accountability mechanisms to fight impunity[48].

Whenever possible, legislation should be technology neutral, so that its applicability is not eroded by future technological developments[49].

The effective implementation of legislation requires governments to put in place complementary measures, including awareness-raising and social mobilization initiatives, education efforts and campaigns, and capacity-building of professionals working with and for children.

In developing appropriate law, it is also important to bear in mind that children are not a homogeneous group. Different responses may be required for children of different age groups, as well as children who have specific needs or who are at heightened risk of being harmed in or through the digital environment.

---

47 Special Representative of the Secretary-General on Violence against Children, *Annual Report of the Special Representative of the Secretary-General on Violence against Children to the Human Rights Council,* A/HRC/31/20 (January 2016), para. 103 and 104.

48 Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), p. 55.

49 Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), p. 64.

Governments should create a clear and predictable legal and regulatory environment which supports businesses and other third parties to meet their responsibilities to safeguard children's rights throughout their operations, at home and abroad[50].

The following aspects will be helpful for policy-makers in reviewing the scope of any legal frameworks and provision of the following:

- grooming or other forms of remote enticement, extortion or coercion of children into inappropriate sexual contact or sexual activity;
- ensuring the possession, production and distribution of CSAM, irrespective of the intent to distribute;
- harassment, bullying, abuse or hate speech online;
- online terrorist material;
- cybersecurity;
- reflection that what is illegal offline is equally illegal online.

4.1.2 Policy and institutional frameworks

Guaranteeing the realization of children's rights in the digital environment requires governments to strike a balance between maximizing the benefits of children's use of ICTs and minimizing the risks associated with them. This can be achieved by including measures to protect children online in the national broadband plans[51] and by developing a separate multifaceted child online protection strategy. Such an agenda should be fully integrated with any existing policy frameworks relevant to children's rights or child protection and should furthermore complement national child protection policies by offering a specific framework for all risks and potential harms for children aiming at creating a safe, inclusive and empowering digital environment[52].

Governments should put in place a national coordinating framework with a clear mandate and sufficient authority to coordinate all activities related to children's rights and digital media and ICTs at cross-sectoral, national, regional, and local levels. Governments should include time-bound goals and a transparent process to evaluate and monitor progress and must ensure that the necessary human, technical and financial resources are made available for the effective operation of this framework[53].

Governments should establish a multi-stakeholder platform to steer the development, implementation and monitoring of the national digital agenda for children. Such a platform should bring together representatives of the most important constituencies, including: children and young people; associations of parents/caregivers; the relevant sections of government; the education, justice, health and social care sectors; national human rights institutions and relevant regulatory bodies; civil society; industry; academia; and relevant professional associations.

---

50 UN Committee on the Rights of the Child, *General Comment No. 16*, para. 53.

51 The State of the Broadband 2019, Recommendation 5.6, page 78. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

52 For model provisions on child protection for national broadband plans see chapter 10 of the Child Online Safety Report.

53 Special Representative of the Secretary-General on Violence against Children, *Annual Report of the Special Representative of the Secretary-General on Violence against Children* (December 2014) A/HRC/28/55 and *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), para. 88.

4.1.3 Regulatory framework

Governments are responsible for infringements of children's rights caused or contributed to by business enterprises where it has failed to undertake necessary, appropriate and reasonable measures to prevent and remedy such infringements or otherwise collaborated with or tolerated the infringements[54].

The Guiding Principles on Business and Human Rights anticipate that corporations should provide remedial and grievance mechanisms that are legitimate, accessible, predictable, equitable, rights-compatible, transparent, based on dialogue and engagement, and a source of continuous learning. Grievance mechanisms established by business enterprises can provide flexible and timely alternative solutions and at times it may be in a child's best interests for concerns raised about a company's conduct to be resolved through them. In all cases, access to courts or judicial review of administrative remedies and other procedures should be available[55]. Consideration should be given to mechanisms that create safe, age-appropriate services for children for users to report their concerns.

Notwithstanding the existence of internal grievance mechanisms, governments should establish monitoring mechanisms for the investigation and redress of children's rights violations, with a view to improving accountability of ICT and other relevant companies, as well as strengthen regulatory agency responsibility for the development of standards relevant to children's rights and ICTs[56]. This is especially important because other remedies available to those adversely affected by corporate action – such as civil proceedings and other judicial redress - are often cumbersome and expensive[57].

The UN Committee on the Rights of the Child has highlighted the potential role of national human rights institutions in this area, by outlining how they could have the role of receiving, investigating and mediating complaints of violations by industry entities; conducting public inquiries into large-scale abuses; and undertaking legislative reviews to ensure compliance with the Convention on the Rights of the Child. The Committee has indicated that, where necessary, "States should broaden the legislative mandate of national human rights institutions to accommodate children's rights and business". It is especially important that any complaints-mechanism be child-sensitive, ensure the privacy and protection of victims, and undertake monitoring, follow-up and verification activities for child victims.

One example of an area in which a national human rights institution or other regulatory body could provide an effective remedy to children is in cases of cyberbullying. Internal remedial and grievance mechanisms at times prove ineffective in such cases because, although the content is distressing and harmful, it is often not addressed by national legislation and there is no clear basis for seeking its removal by the content host. Empowering a public authority to receive complaints regarding cases of cyberbullying and to intercede with content hosts to have the relevant material removed would be an important safeguard for children[58]. It would have the

54 UN Committee on the Rights of the Child, *General Comment No.* 16, para. 28.
55 Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, A/HRC/17/31 (2011), para. 71.
56 UN Committee on the Rights of the Child, *Report of the 2014 Day of General Discussion*, para. 96.
57 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016), para. 71.
58 Bertrand de Crombrugghe, "Report of the Human Rights Council on Its Thirty-First Session" (UN Human Rights Council, 2016).

advantages of providing a rapid response – which is of crucial importance in the context of cyberbullying - and also a clear legal basis for addressing the removal of cyberbullying material.

In framing its approach to regulation of the digital environment, governments must also be cognisant of the impact of such regulation on the enjoyment of all human rights, including freedom of expression[59].

Governments should place an obligation on businesses to undertake child-rights due diligence. This would ensure that business enterprises identify, prevent and mitigate their impact on children's rights including across their business relationships and within global operations[60].

In addition, governments should consider complementary measures such as ensuring that industry entities whose activities may have an impact on children's rights in the digital environment must comply with the highest standards in terms of preventing and responding to potential rights violations in order to qualify for funding or contracts.

4.2 Recommendations for implementation

Governments should ensure access to effective remedies for child victims of rights violations, including assistance to seek prompt and appropriate reparation for the harm suffered, through compensation where appropriate. Governments should also provide adequate support and assistance for child victims of violations related to digital media and ICTs, including comprehensive services to ensure the child's full recovery and reintegration, and prevent re-victimization of child victims[61].

Safe and easily accessible child-sensitive counselling, reporting and complaint mechanisms, such as helplines, should be established by law and should form part of the national child protection system. It is important to ensure that these services are connected to any regulatory services to help streamline a child's interactions with institutional bodies during a time that they may be experiencing distress. Helplines are particularly valuable with respect to highly sensitive issues, such as sexual abuse, which children may find difficult to discuss with peers, parents, caregivers or teachers. Helplines also play a crucial role in directing children to services such as legal services, safe houses, law enforcement or rehabilitation[62].

Also, governments needs to understand and track offender's behaviour to increase the detection rates of abusers and reduce the risk of convicted abusers to reoffend. Establishing helplines offering free and anonymous phone or chat-based counselling and support for people who experience feelings or thoughts of sexual interest in children – potential offenders. Helping offenders change their behaviour minimize the risk of reoffending.

Statutory complaints-handling mechanisms also form a crucial part of the framework for effective remedies.

Regulators should conduct independent measurements and studies to assess how platforms report and deal with issues concerned with child protection. Technology exists for regulators

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

to independently monitor platforms. Industry providers should be supported to publish transparency reports.

Together with the international community and the industry, governments should develop a universal set of metrics that stakeholders can use to measure all relevant aspects of child online safety.

4.2.1 Sexual exploitation

Concrete considerations for policy-makers when considering threats to children of harms, specifically child sexual abuse material, self-generated content, grooming and sextortion and other online risks. These might include:

- Steps to disrupt or reduce the traffic in CSAM, for example by establishing a national hotline or an IWF Reporting Portal, and by deploying measures that will block access to online content known to contain or advertise the availability of CSAM.
- Ensuring that national processes are in place to ensure all CSAM found in a country is channelled towards a centralised, national resource that has legislative powers to direct companies to remove content.
- Strategies to address the demand for CSAM particularly among those who have convictions for such offences. It is important to build awareness of the fact that this is not a victimless crime: children are abused to produce the material being viewed and by intentionally viewing or downloading CSAM one is contributing directly to the abuse of the child depicted and one is also encouraging the abuse of more children to produce more pictures.
- Building awareness of the fact that children can never consent to being sexually abused, whether for the production of CSAM or in any other way. Encourage people who use CSAM to seek help, while at the same time, making them aware that they will be held criminally responsible for the illegal activity in which they engaged/are engaging.
- Other strategies to address the demand for CSAM. For example, some countries maintain a register of convicted sex offenders. Courts have issued judicial orders banning such offenders from using the Internet altogether or from using parts of the Internet that are frequented by children and young people. The problem with these orders hitherto has been one of enforcement. However, in some countries, consideration is being given to integrating the list of known sex offenders into a block list that will prevent those on it from visiting or joining certain web sites, for example web sites known to be visited by large numbers of children and young people. Of course, if the offender joins a web site while using a different name or fake log-in the effectiveness of such measures can be greatly reduced but by criminalising this behaviour a further deterrent can be established.
- Providing appropriate long-term support for victims. Where children or young people have been victimized online, where for example an illegal image of them has appeared on the Internet, they will naturally feel very concerned about who might have seen it and what impact this will have on them. It could leave the child or young person feeling vulnerable to bullying or to further sexual exploitation and abuse. In that context it will be important for there to be professional support services available to support children and young people who find themselves in these circumstances. Such support may need to be provided on a long-term basis.
- Ensuring that a mechanism is established and is widely promoted to provide a readily understood and rapid means for reporting illegal content or illegal or worrying online behaviour e.g. a system similar to that which has been established by the Virtual Global Taskforce and INHOPE. The use of the INTERPOL i24/7 system should be encouraged.
- Ensuring that a sufficient number of law enforcement officials are appropriately trained in investigating Internet and computer-based crime and have access to appropriate forensic facilities to enable them to extract and interpret relevant digital data.

- Investing in training for law enforcement, prosecutorial and judicial authorities in the methods used by online criminals to perpetrate these crimes. Investment will also be needed in acquiring and maintaining the facilities necessary to obtain and interpret forensics evidence from digital devices. In addition, it will be important to establish bilateral and multilateral collaboration and information exchanges with relevant law enforcement authorities and investigative bodies in other countries.

4.2.2 Education

Educate children on digital literacy as part of a strategy to ensure they can benefit from technology, free from harm. This will allow children to develop critical thinking skills that will help them to identify and understand the good and bad sides of their behaviour in the digital space. Whilst it is important to illustrate to children the harms that can occur online, this will only be effective if included as part of a broader digital literacy programme that should be age appropriate and focus on skills and competencies. It is important to include social and emotional learning concepts within online safety education as these will support students' understanding and management of emotions to have healthy and respectful relationships, both online and offline.

Children should have appropriate tools and knowledge to address the Internet is one of the best ways to keep them safe. Introducing digital literacy in the school curriculums is one way. Another possibility is to create educational resources outside of the school curriculum.

Those working with children should have suitable knowledge and skills to confidently support children in both responding to and resolving child online protection related issues as well as providing children with the necessary digital skills to successfully benefit from technology.

4.2.3 Industry

National and international industry players should work to raise awareness of the issues around child online safety and to help all the adults responsible for a child's wellbeing – including parents and caregivers, schools, youth serving organizations and communities – develop the knowledge and skills they need to keep children safe. Industry should adopt a safer by design approach to their products, services and platforms, recognising safety as a core objective.

- Provide age appropriate family friendly tools to help their users to better manage the protection of their families online.
- Provide suitable reporting mechanisms for their users to report issues and concerns. Users should expect timely responses these reports with information about actions taken and, if applicable, where users can obtain further support.
- Additionally, provide proactive reporting of abuse against children to detect and address any sort of abuse (classified as criminal activity) against children. This practice has shown that if all the stakeholders contribute to detect, block and report we can think in having a cleaner and safer Internet for all. Industry should consider taking all relevant tools to prevent their platforms being exploited, such as the IWF Services.

It is vital to engage all the relevant actors in the ecosystem should be aware of the online risks and harms to be able to prevent children from being exposed to unnecessary risks.

Develop common metrics for child online safety to measure all relevant aspects of the matter. Common standards and metrics are the only way to track progress in countries and to determine success of the projects and activities implemented to eliminate any violence against children and acknowledge the strength of the child online safety ecosystem.

5. Developing a national child online protection strategy

5.1 A national checklist

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

Table 1: Key areas for consideration

	#	Key areas for consideration	Further details
Legal framework	1	Review the existing legal framework to determine that all necessary legal powers exist to enable law enforcement and other relevant agencies to protect persons under the age of 18 online on all Internet-enabled platforms.	It will generally be necessary for there to be in place a body of laws which makes it clear that any and every crime that can be committed against a child in the real world can, *mutatis mutandis*, also be committed on the Internet or on any other electronic network. It may also be necessary to develop new laws or adapt existing ones to outlaw certain types of behaviour which can only take place on the Internet, for example the remote enticement of children to perform or watch sexual acts, or grooming children to meet in the real world for a sexual purpose. Ancillary to these purposes it will generally be necessary for there to be in place a legal framework which outlaws the misuse of computers for criminal ends, outlaws hacking or other malicious or non-consensual use of computer code and establishes that the Internet is a locus within which crimes can be committed.
	2	Establish, *mutatis mutandis*, that any act against a child which is illegal in the real world is illegal online and that the online data protection and privacy rules for children are also adequate.	

	#	Key areas for consideration	Further details
Regulatory framework	3	Consider the regulatory policy development. This may include a self or co-regulatory policy development as well as a full regulatory framework. The self or co-regulatory model might include the formulation and publication of codes of good practice or basic online safety expectations, both in terms of helping to engage, coordinate or orchestrate and sustain the involvement of all relevant stakeholders and in terms of enhancing the speed with which appropriate responses to technological change can be formulated and put into effect. A regulatory model might define the expectations and obligations across stakeholders and enshrine within a legal context. Penalties for policy infringement may also be considered.	Some countries have established a self or co-regulatory model in relation to developing policy in this area and through such models they have, for example, published codes of good practice to guide the Internet industry in terms of the measures which may work best when it comes to keeping children and young people safer online. For example within the European Union where EU-wide codes have been published both for social networking sites and mobile phone networks in relation to the provision of content and services to children and young people via their networks. Self and co-regulation can be more agile in terms of enhancing the speed with which appropriate responses to technological change can be formulated and put into effect. More recently several countries have developed and/or implemented a regulatory framework. In these examples, the regulatory framework has emerged from self or co regulatory models and defines the requirements and expectations for stakeholders, particularly industry providers, to better protect their users.

	#	Key areas for consideration	Further details
Reporting - illegal content	4	Ensure that a mechanism is established and is widely promoted to provide readily understood means for reporting the variety of illegal content found on the Internet. For example, a national hotline, which has the capacity to respond rapidly and have illegal material removed or rendered inaccessible. Industry should have mechanisms to identify, block and remove abuse of children online, taking all services relevant to their organisations.	Mechanisms for reporting abuse of an online service or for reporting objectionable or illegal behaviour online, for example to a national hotline, should be widely advertised and promoted both on the Internet and in other media. If a national hotline is not available, the IWF offers the Reporting Portals solution. Links to report abuse mechanisms should be prominently displayed on relevant parts of any web site that allows user generated content to appear. It should also be possible for people who feel threatened in any way, or for people who have witnessed any worrying activity on the Internet, to be able to report it as quickly as possible to the relevant law enforcement agencies who need to be trained and ready to respond. The Virtual Global Taskforce is a law enforcement body which provides a 24/7 mechanism to receive reports about illegal behaviour or content from persons in the USA, Canada, Australia and Italy, with other countries expected to join soon. See www.virtualglobaltaskforce.com. See also INHOPE.
Reporting - user concerns	5	Industry should provide users with the opportunity to report concerns and issues to their users and respond accordingly.	Providers should be obligated to provide, and clearly signpost, their users with the ability to report issues and concerns within their services. These should be child friendly and readily available.

	#	Key areas for consideration	Further details
Actors and stakeholders	6	Engage all the relevant stakeholders with an interest in online child protection, in particular: • Government agencies • Law enforcement • Social services organizations • Internet Service Providers (ISPs) and other Electronic Service Providers (ESPs) • Mobile phone network providers • Public Wi-Fi providers • Other relevant hi-tech companies • Teacher organizations • Parent organizations • Children and young people • Child protection and other relevant NGOs • Academic and research community • Owners of Internet cafés and other public access providers e.g. libraries, telecentres, PC Bangs[63] and online gaming centres etc.	Several national governments have found it useful to bring together all of the key stakeholders and players to focus on developing and implementing a national initiative around making the Internet a safer place for children and young people, and raising awareness of the issues and how to deal with them in a very practical way. It will be important within this strategy to appreciate that many are universally and constantly connected to the Internet via a variety of devices. The broadband, mobile and Wi-Fi operators need to be involved. Additionally, in many countries the network of public libraries, telecentres and Internet cafes can be important sources of Internet access particularly for children and young people.
Research	7	Undertake research of the spectrum of national actors and stakeholders to determine their opinions, experiences, concerns and opportunities with regards to child online protection. This should also appreciate the extent of any responsibility together with existing or planned activities to protect children online.	

[63] A "PC Bang" is term commonly used in the Republic of Korea and in some other countries to describe a large room where a LAN facilitates large scale game playing, either online or between players in the room.

	#	Key areas for consideration	Further details
Education digital literacy and competency	8	Develop digital literacy features as part of any national school curriculum that is age appropriate and applicable to all children.	Schools and the education system generally will represent the foundation of the education and digital literacy component of a national child online protection strategy. Any national school curriculum should include child online protection aspects and aim to provide children of all ages with age appropriate skills to both benefit and successfully use technology and to be sensitive as to the threats and harms to successfully avoid. It should recognise and reward positive and constructive online behaviours. Within any education and awareness campaign it will be important to strike the right tone. Fear-based messaging should be avoided, and due prominence should be given to the many positive and fun features of the new technology. The Internet has great potential as a means of empowering children and young people to discover new worlds. Teaching positive and responsible forms of online behaviour is a key objective of education and awareness programmes. Those working with children, especially teachers, should be suitably trained and equipped to successfully educate and provide children with these skills. They should understand the online threats and harms together with the ability to confidently recognise the signs of abuse and harm and to respond and report these concerns to protect their children

	#	Key areas for consideration	Further details
Educational resources	9	Draw on the knowledge and experience of all stakeholders and develop Internet safety messages and materials which reflect local cultural norms and laws and ensure that these are efficiently distributed and appropriately presented to all key target audiences. Consider enlisting the aid of the mass media in promoting awareness messages. Develop materials which emphasise the positive and empowering aspects of the Internet for children and young people and avoid fear-based messaging. Promote positive and responsible forms of online behaviour. Consider developing resources to help parents assess their own children's online safety and learn about how to minimize risks and maximize potential for their own family through targeted education.	When producing educational materials, it is important to bear in mind that many people who are new to the technology will not feel comfortable using it. For that reason, it is important to ensure that safety materials are made available in either written form or produced using other media with which newcomers will feel more familiar, for example, with video Many of the large Internet companies produce web sites which contain a great deal of information about online issues for children and young people. However, very often this material will only be available in English or in a very narrow band of languages. It is very important, therefore, that materials are produced locally which reflect local laws as well as local cultural norms. This will be essential for any Internet safety campaign or any training materials that are developed.
Child protection	10	Ensure that universal and systematic child protection mechanisms are in place that oblige all those working with children (social care, health, schools etc.) to identify, respond and report incidents of abuse and harm that occur online.	A universal child protection system should be in place and applicable to all those working with children, obliging them to report child abuse or harm to allow the situations to be investigated and resolved.

	#	Key areas for consideration	Further details
National awareness	11	Organise national awareness campaigns to create the opportunity to universally highlight child online protection issues. It may be beneficial to harness global campaigns such as Safer Internet Day to build a campaign.	Parents, guardians, and professionals, such as teachers, have a crucial role to play in helping to keep children and young people safer online. Supportive programmes should be developed which help build awareness of the issues and also provide strategies for dealing with them. Consideration should also be given to enlisting the aid of the mass media in promoting awareness messages and campaigns. Opportunities such as Safer Internet Day will be helpful in stimulating and encouraging a national dialogue about child online protection. Many countries have successfully built national awareness campaigns anchored around Safer Internet Day and involve the full array of actors and stakeholders in amplifying universal messaging across media and social media

	#	Key areas for consideration	Further details
Tools, services, and settings	12	Consider the role of device settings, technical tools (such as filtering programmes) and child protection apps and settings that can help. Encourage users to take responsibility for their devices by encouraging updates of the operating system plus the use of suitable security software and apps.	There are several services available which can help screen out unwanted material or block unwanted contacts. Some of these child safety and filtering programmes may be essentially free because they are part of a computer operating system or they are provided as part of a package available from an ISP or ESP. The manufacturers of some game consoles also provide similar tools if the device is Internet enabled. These programmes are not fool-proof but they can provide a welcome level of support, particularly in families with younger children. The majority of devices are provided with settings that help to protect children and also promote healthy and balanced use. This extends to mechanisms that allow parents to manage their children's devices, allocating time, the apps and services that they are able to use and manage an purchases. More recently reports and settings have been developed to enable users and parents to better understand and manage screen time and access. These technical tools should be used as part of a broader arsenal. Parental and/or guardian involvement is critical. As children start getting a bit older they will want more privacy and they will also feel a strong desire to start exploring on their own. In addition, where a billing relationship exists between vendor and customer, age verification processes can play a very valuable role in helping vendors of age restricted goods and services or the publishers of material which is intended only for audiences at or above a certain age, to reach out to those specific audiences. Where no billing relationship exists the use of age verification technology may be problematic or in many countries it may be impossible due to a lack of reliable data sources.

5.2 Example questions

With the identification of the national stakeholders and actors, the following questions may be circulated to stakeholders and actors and invite them to complete and respond. Their responses will help to determine the extent of policy coverage, the strengths as well as the areas to focus on across a national checklist.

- To what extent is online safety and children's rights your responsibility?
- How is online safety and children's rights integrated into your existing policies and processes?
- To what extent is online safety covered within existing legislation?
- What are your online safety priorities?
- What activities do you have to support online safety?
- How do you work with other agencies and organisations to improve/progress online safety?
- Can children/parents report online safety concerns or issues to you?
- What are your three key challenges in the online world?
- What are your three key opportunities in the online world?

It would also be helpful to undertake research and understanding the perception and experiences of children as well as their parents with regards child online protection.

6. Reference material

Child online safety: Key documents and publications

2020

- ECPAT International, Sexual Exploitation Of Children In The Middle East And North Africa, 2020
- DQ Institute, 2020 Child Online Safety Report, 2020
- EU Kids Online, EU Kids Online 2020: Survey results from 19 countries, 2020

2019

- Internet Watch Foundation (IWF), Annual Report, 2019
- WeProtect Global Alliance, Global Threat Assessment, 2019
- Broadband Commission / ITU, Child Online Safety. Universal Declaration, 2019
- Broadband Commission / ITU, Child Safety Online: Minimizing the Risk of Violence, Abuse and Exploitation Online, 2019
- Global Kids Online, Growing up in a connected world, 2019
- Rethinking the Detection of Child Sexual Abuse Imagery on the Internet, in Proceedings of the 2019 World Wide Web Conference, May 13–17, 2019, San Francisco, USA, 2019
- UK Home Office, Online Harms White Paper (UK only), 2019
- PA Consulting, A tangled web: rethinking the approach to online CSEA, 2019
- UK Information Commissioner Office, Consultation on Code of Practice to help protect children online (UK only), 2019
- Global Fund to End Violence against Children, Disrupting Harm: evidence to understand online child sexual exploitation and abuse, 2019
- Global Partnership to End Violence against Children, Safe to Learn Call for Action, Youth Manifesto, 2019
- UNESCO, Behind the numbers: Ending school violence and bullying, 2019 (includes data on online hurtful behaviour and cyber-bullying)
- United Nations Human Rights, children's rights in relation to the digital environment, 2019
- Australian eSafety Commissioner, Safety by Design Overview, 2019
- UNICEF, Why businesses should invest in digital child safety brief, 2019
- U.S. Department of State, Trafficking in Persons report, 2019

2018

- WeProtect Global Alliance, Global Threat Assessment, 2018
- Child Dignity on the Digital World, Technical Working Group Report, 2018 Council of Europe, Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- Global Fund to End Violence against Children, Two years of supporting solutions: results from the Fund's investments, 2018
- WeProtect Global Alliance, Country examples of Model of National Response capabilities and implementation, 2018
- INTERPOL and ECPAT International, Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, 2018
- EUROPOL, Internet Organized Crime Threat Assessment (IOCTA), 2018
- NetClean, Report about Child Sexual Abuse Cybercrime, 2018

- International Centre for Missing & Exploited Children (ICMEC), Child Sexual Abuse Material: Model Legislation & Global Review, 9th Edition, 2018
- International Centre for Missing & Exploited Children (ICMEC), Studies in Child Protection: Sexual Extortion and Non-Consensual Pornography, 2018
- International Association of Internet Hotlines, INHOPE Report, 2018
- Internet Watch Foundation (IWF), Annual Report, 2018
- Thorn, Production and Active Trading of Child Sexual Exploitation Images, 2018
- ITU, Global Cybersecurity Index, 2018
- CSA Centre of Expertise, Interventions for perpetrators of online child sexual exploitation - a scoping review and gap analysis, 2018
- NatCen, Behaviour and Characteristics of Perpetrators of Online-facilitated CSEA - a rapid evidence assessment, 2018
- UNICEF, Policy guide on children and digital connectivity, 2018

2017

- The National Center for Missing & Exploited Children (NCMEC), The online enticement of children: an in-depth analysis of CyberTipline Reports, 2017
- 5Rights Foundation, Digital Childhood, development milestones in digital environment, 2017
- Childnet, DeShame Report, 2017
- Canadian Centre for Child Protection, Survivors' survey, 2017
- Internet Watch Foundation (IWF), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review, 2017
- Thorn, Sextortion online survey with 2,097 victims of sextortion ages 13 to 25, 2017
- UNICEF, Children in a Digital World, 2017
- Western Sydney University, Young and Online: Children's Perspectives on Life in Digital Age, 2017
- ECPAT International, Sexual Exploitation of Children in South East Asia, 2017

2016

- UNICEF, Perils and possibilities: growing up online, 2016
- UNICEF, Child protection in the digital age: National responses to online CSEA in ASEAN, 2016
- Centre for Justice and Crime Prevention, Child Online Protection in the MENA Region, 2016
- ECPAT International, Interagency Working Group on Sexual Exploitation of Children, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (The Luxembourg Guidelines), 2016

2015

- WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, 2015
- NCMEC, A Global Landscape of Hotlines Combating CSAM, 2015
- ITU and UNICEF, Guidelines for Industry on Child Online Protection, 2015

Related to human rights in a digital world

- Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- UNESCO, Internet Universality Indicators, 2019
- Ranking Digital Rights (RDR), 2019 RDR Corporate Accountability Index, 2019
- Broadband Commission for Sustainable Development, The State of the Broadband, 2019
- ITU, Measuring Digital Development, 2019
- ITU, Measuring Information Society Report, 2018
- UNICEF, Children and Digital Marketing Industry Toolkit, 2018
- Broadband Commission for Sustainable Development, Digital health, 2017
- Broadband Commission for Sustainable Development, Digital Skills for life and work, 2017
- Broadband Commission for Sustainable Development, Digital gender divide, 2017
- UNICEF, Privacy, protection of personal information and reputation, 2017
- UNICEF, Freedom of expression, association, access to information and participation, 2017
- UNICEF, Access to the Internet and digital literacy, 2017
- UN CRC, Guidelines on effective protection of children from sexual exploitation, 2019

For further resources, please refer to the additional resource list on www.itu-cop-guidelines.com

Appendix 1: Terminology

The definitions below are mainly drawn upon existing terminologies as elaborated in the Convention of the Rights of the Child, 1989, as well as by the Inter-agency working group on child sexual exploitation in the Terminology Guidelines on the Protection of Children from Sexual Exploitation and Sexual Abuse, 2016[64] (Luxembourg Guidelines), by the Council of Europe Convention: Protection of Children against Sexual Exploitation and Sexual Abuse, 2012[65] as well as by the Report Global Kids Online, 2019[66].

Adolescent

Adolescents are people aged 10-19. It is important to note that *adolescents* is not a binding term under international law, and those below the age of 18 are considered to be children, whereas 19 year-olds old are considered adults, unless majority is attained earlier under national law[67].

Artificial intelligence (AI)

In the broadest sense, the term refers indistinctly to systems that are pure science fiction (so-called "strong" AIs with a self-aware form) and systems that are already operational and capable of performing very complex tasks (face or voice recognition, vehicle driving - these systems are described as "weak" or "moderate" AIs)[68].

AI systems

An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments, and are designed to operate with varying levels of autonomy[69].

Best interest of the child

Describes all the elements necessary to make a decision in a specific situation for a specific individual child or group of children[70].

---

64 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse," 2016, 114, http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf.

65 Council of Europe, Conseil de l'Europe, and Council of Europe, Protection of Children against Sexual Exploitation and Sexual Abuse: Council of Europe Convention (Strasbourg: Council of Europe Publishing, 2012), https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf.

66 Globalkidsonline.net, "Done Right, Internet Use Can Increase Learning and Skills," November 2019, http://globalkidsonline.net/synthesis-report-2019/.

67 UNICEF and ITU, Guidelines for Industry on Child Online Protection (itu.int/cop, 2015), https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

68 Council of Europe, "What's AI?," coe.int, Artificial Intelligence, accessed January 16, 2020, https://www.coe.int/en/web/artificial-intelligence/what-is-ai.

69 OECD, "Recommendation of the Council on Artificial Intelligence" (OECD, 2019), https://webcache.googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print%3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari.

70 OHCHR, "Convention on the Rights of the Child," accessed January 16, 2020, https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

Child

In accordance with article 1 of the Convention on the Rights of the Child, a child is anyone under 18 years old, unless majority is attained earlier under national law[71].

Child sexual exploitation and abuse (CSEA)

Describes all forms of sexual exploitation and sexual abuse (CRC, 1989, art. 34), e.g. "(a) the inducement or coercion of a child to engage in any unlawful sexual activity; (b) The exploitative use of children in prostitution on or other unlawful sexual practices; (c) The exploitative use of children in pornographic performances and materials" as well as a "sexual contact that usually involves force upon a person without consent". Sexual exploitation and abuse of children increasingly take place through the Internet, or with some connection to the online environment[72].

Child sexual (exploitation and) abuse material (CSAM)

The rapid evolution of ICTs has created new forms of online child sexual exploitation and abuse, which can take place virtually and does not have to include physical face-to-face meeting with the child[73]. Though many jurisdictions still label images and videos of child sexual abuse 'child pornography' or the 'indecent images of children', these guidelines will refer to the subjects collectively as child sexual abuse material (henceforth, CSAM). This is in accordance with the Broadband Commission Guidelines and the WePROTECT Global Alliance Model National Response[74]. This term more accurately describes the content. Pornography refers to a legitimate, commercialised industry, and as the Luxembourg Guidelines state the use of the term:

"*may (inadvertently or not) contribute to diminishing the gravity of, trivialising, or even legitimising what is actually sexual abuse and/or sexual exploitation of children […] the term 'child pornography' risks insinuating that the acts are carried out with the consent of the child, and represent legitimate sexual material*"[75].

The term CSAM refers to material that represents acts that are sexually abusive and/or exploitative to a child. This includes, but is not limited to, material recording the sexual abuse of children by adults; images of children included in sexually explicit conduct; the sexual organs of children when the images are produced or used for primarily sexual purposes.

---

71 OHCHR; UNICEF and ITU, *Guidelines for Industry on Child Online Protection*.

72 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

73 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse"; UNICEF, "Global Kids Online Comparative Report (2019)."

74 WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Absue (CSEA): A Model National Response.," 2016, https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf; Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)."

75 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

Children and young people

Describes all person under the age of 18 years wherein children, also referred to as younger children in the guidelines covers all person under the age of 15 years and young people comprise of the 15 to 18 years age group.

Connected toys

Connected toys connect to the Internet using technologies such as Wi-Fi and Bluetooth, and typically operate in conjunction with companion apps to enable interactive play for children. According to Juniper Research, in 2015 the market for connected toys reached USD 2.8 billion and is predicted to increase to USD 11 billion by 2020. These toys collect and store personal information from children including names, geolocation, addresses, photographs, audio, and video recordings[76].

Cyberbullying, also referred to as Online bullying

International law does not define cyberbullying. For the purpose of this document, cyberbullying is described an intentional aggressive act carried out repeatedly by either a group or an individual using digital technology and targeting a victim who cannot easily defend themselves[77]. It usually involves "using digital technology and the internet to post hurtful information about someone, purposely sharing private information, photos or videos in a hurtful way, sending threatening or insulting messages (via email, instant messaging, chat, texts), spreading rumours and false information about the victim or purposely excluding them from online communications"[78]. It may involve direct (such as chat or text messaging), semi-public (such as posting a harassing message on an e-mail list) or public communications (such as creating a website devoted to making fun of the victim).

Cyberhate, discrimination, and violent extremism

"Cyberhate, discrimination and violent extremism are a distinct form of cyber violence as it is targeting a collective identity, rather than individuals […] often pertaining to race, sexual orientation, religion, nationality or immigration status, sex/gender, and politics"[79].

Digital citizenship

Digital citizenship refers to the ability to engage positively, critically and competently in the digital environment, drawing on the skills of effective communication and creation, to practice forms of social participation that are respectful of human rights and dignity through the responsible use of technology[80].

---

76 Jeremy Greenberg, "Dangerous Games: Connected Toys, COPPA, and Bad Security," Georgetown Law Technology Review, December 4, 2017, https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/.

77 Anna Costanza Baldry, Anna Sorrentino, and David P. Farrington, "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities," Children and Youth Services Review 96 (January 2019): 302–7, https://doi.org/10.1016/j.childyouth.2018.11.058.

78 UNICEF, "Global Kids Online Comparative Report (2019)"; "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

79 UNICEF, "Global Kids Online Comparative Report (2019)."

80 Council of Europe, "Digital Citizenship and Digital Citizenship Education," Digital Citizenship Education, accessed January 16, 2020, https://www.coe.int/en/web/digital-citizenship-education/home.

Digital literacy

Digital literacy means having the skills one needs to live, learn, and work in a society where communication and access to information is increasingly through digital technologies like Internet platforms, social media, and mobile devices[81]. It includes clear communication, technical skills and critical thinking.

Digital resilience

This term describes a child's capacity to emotionally cope with harms encounters online. Digital resilience included having the emotional resources needed to understand when the child is at risk online, know what to do to seek help, learn from experience and to recover when things go wrong[82].

Educators

An educator is a person who systematically works to improve another person's understanding of a given subject. The role of educators encompasses both those who teach in classrooms and the more informal educators who, for example, those who use social networking sites platforms and services to provide online safety information or run community or school based courses to enable children and young people to stay safe online.

The work of educators will vary depending on the context in which they work and the age group of the children and young people (or adults) they seek to educate.

Grooming/online grooming

Grooming/online grooming as defined in the Luxembourg Guidelines, refers to the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or online sexual contact with that person persuading the child to have a sexual relationship[83]. A process intended to lure children into sexual behaviour or conversations with or without their knowledge, or a process that involves communication and socialization between the offender and the child in order to make him or her more vulnerable to sexual abuse. The term grooming has not been defined in international law; some jurisdictions, including Canada, use the term 'luring'.

Information and communication technologies (ICTs)

Information and communication technologies describe all information technologies that stress the aspect of communication. This includes all Internet-connecting services and devices such as among others computer, laptops, tablets, smartphones, game consoles, televisions and watches[84]. It further includes services such as radio as well as among others broadband, network hardware and satellite systems.

---

81 Western Sydney University-Claire Urbach, "What Is Digital Literacy?," accessed January 16, 2020, https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy.

82 Dr. Andrew K. Przybylski, et al., "A Shared Responsibility. Building Children's' Online Resilience Report" (ParentZone, University of Oxford and Virgin Media, 2014), https://parentzone.org.uk/sites/default/files/Building%20Online%20Resilience%20Report.pdf.

83 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

84 UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*

Internet and associated technologies

It is now possible to connect to the Internet using a variety of different devices, e.g., smartphones, tablets, games consoles, TVs and laptops as well as more traditional computers. Thus, except where the context suggests otherwise, any reference to the Internet should be understood to encompass all of these different methods. To encompass the Internet's rich and complex tapestry, 'Internet and associated technologies', 'ICT and online industries' and 'Internet-based services' are used interchangeably.

Notice and takedown

Operators and service providers are sometimes notified of suspect content online by customers, members of the public, law enforcement or hotline organizations. Notice and takedown procedures refer to a company's processes for the swift removal ('takedown') of illegal content (illegal content being defined according to the jurisdiction) as soon as they have been made aware ('notice') of its presence on their services.

Online gaming

'Online gaming' is defined as playing any type of single or multiplayer commercial digital game via any Internet-connected device, including dedicated consoles, desktop computers, laptops, tablets and mobile phones.

The 'online gaming ecosystem' is defined to include watching others play video games via e-sports, streaming or video-sharing platforms, which typically provide options for viewers to comment on or interact with the players and other members of the audience[85].

Parental control tools

Software that allows users, typically a parent, to control some or all functions of a computer or other device that can connect to the Internet. Typically, such programmes can limit access to particular types or classes of websites or online services. Some also provide scope for time management, i.e., the device can be set to have access to the Internet only between certain hours. More advanced versions can record all texts sent or received from a device. The programmes normally will be password protected[86].

Parents, carers, guardians

Several Internet sites refer to parents in a generic way (such as on a "parents' page" and refer to "parental controls") Therefore it might be useful to define the people who ideally should empower children to maximise the opportunities available online, ensure that children and young people use Internet sites safely and responsibly and grant their consent to have access to specific Internet sites. In this document, the term "parents" refers to anyone (excluding educators) who has a legal responsibility for a child. Parental responsibility will vary from country to country as will legal parental rights.

---

85 UNICEF, "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry," DISCUSSION PAPER SERIES: Children's Rights and Business in a Digital World, 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

86 UNICEF and ITU, *Guidelines for Industry on Child Online Protection*.

Personal information

The term describes individually identifiable information about a person, that is collected online. This includes the full name, contact details like home and email addresses, phone numbers, fingerprints or facial recognition material, insurance numbers or any other factor, that permits the physical or online contacting or localisation of a person. In this context it further refers to any information about a child and his or her entourage that is collected online by service providers online, including connected toys and the Internet of things and any other connected technology.

Privacy

Privacy is often measured in terms of sharing personal information online, having a public social media profile, sharing information with people they got to know online, using privacy settings, sharing passwords with friends, being concerned about privacy[87].

Sexting

Sexting is commonly defined as the sending, receiving, or exchanging of self-produced sexualised content including images, messages, or videos through mobile phones and/or the Internet[88]. The creation, distribution and possession of sexual images of children is illegal in most countries. If sexual images of children are disclosed, adults should not view them. The sharing of sexual images by an adult with a child is always a criminal act and that between children harm can occur and reporting and actions to remove shared images may be needed.

Sextortion or sexual extortion of children

Sextortion describes or sexual extortion (also referred to as "online sexual coercion and extortion")[89] "blackmailing of a person with the help of self-generated images of that person in order to extort sexual favours, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted person (e.g., posting images on social media)"[90].

The Internet of Things (IoT)

Internet of Things represents the next step towards the digitisation of society and the economy, where objects and people are interconnected through communication networks and report about their status and/or the surrounding environment[91].

URL

The abbreviation stands for 'uniform resource locator', the address of an Internet page[92].

---

87 "Children's Online Privacy Protection Act," Pub. L. No. 15 U.S.C. 6501-6505 (1998), https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

88 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

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

90 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

91 Ntantko, The Internet of Things, 1 October 2013, Digital Single Market - European Commission, https://ec.europa.eu/digital-single-market/en/internet-of-things.

92 UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*

Virtual reality

Virtual reality is the use of computer technology to create the effect of an interactive three-dimensional world in which the objects have a sense of spatial presence[93].

Wi-Fi

Wi-Fi (Wireless Fidelity) is the group of technical standards that enable data transmission over wireless networks[94].

[93] NASA, "Virtual Reality," nas.nasa.gov, accessed January 16, 2020, https://www.nas.nasa.gov/Software/VWT/vr.html.

[94] Children's Online Privacy Protection Act.

Appendix 2: Contact offences against children and young people

Children and young people can be exposed to a range of unwanted or inappropriate contact on the Internet that can have dire consequences for them. Some of this contact might be sexual in nature.

Studies have shown that 22 per cent have been bullied[95], harassed or stalked online; 24 per cent have received unwanted sexual comments;[96] 8 per cent have met people in real life whom they had previously only known online[97]. Though the rates vary by country and region, these figures demonstrate that the risks are real[98]. One Internet study in the United States of America[99] found that 32 per cent of teenagers online have been contacted by a complete stranger, of those, 23 per cent said they felt scared and uncomfortable during the contact; and 4 per cent had received aggressive sexual solicitation.

Sexual predators use the Internet to contact children and young people for sexual purposes, often using a technique known as grooming whereby they gain the child's confidence by appealing to his or her interests. They often introduce sexual topics, photos and explicit language to desensitize, raise sexual awareness and soften the will of their young victims. Gifts, money and even tickets for transportation are used to persuade and lure the child or young person to a place where the predator can sexually exploit him or her. These encounters may even be photographed or videotaped. Children and young people often lack emotional maturity and self-esteem, which makes them susceptible to manipulation and intimidation. They are also hesitant to tell adults about their encounters for fear of embarrassment or of losing access to the Internet. In some cases, they are threatened by predators and told to keep the relationship a secret. Sexual predators also learn from each another through Internet fora and chat rooms.

95 U-report (2019), http://www.ureport.in/v2/.
96 Project deSHAME (2017), https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf.
97 Lenhardt, A., Anderson, M., Smith, A. (2015), Teens, Technology and Romantic Relationships, https://www.pewresearch.org/internet/2015/10/01/teens-technology-and-romantic-relationships/
98 Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/.
99 Amanda Lenhart et al., "The Use of Social Media Gains a Greater Foothold in Teen Life as They Embrace the Conversational Nature of Interactive Online Media.," *Pew Internet and American Life Project*, 2007, 44, https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

Appendix 3: The WeProtect Global Alliance

The WePROTECT Model National Response

The WePROTECT Global Alliance strategy supports countries to develop coordinated multi-stakeholder responses to tackle online child sexual exploitation, guided by its Model National Response (MNR). The WPGA Model National Response acts as a blueprint for national action. It provides a framework for countries to draw upon to tackle online child sexual exploitation (OCSE). The model is intended to help a country to:

- evaluate its current response to OCSE and identify gaps;
- prioritise national effort on filing gaps;
- enhance international understanding and cooperation.

The Model does not seek to prescribe activities or set out a single approach. Its purpose is to describe the capabilities needed for effective child protection and to support countries to develop or enhance their existing capabilities. It also lists a number of enablers which, if in place and effective will accelerate and improve outcomes. The MNR includes twenty-one capabilities, divided into six sections: policy and governance, criminal justice, victim, societal, industry and media and communications. The WPGA believes that action in all six areas will deliver a complete national response to this crime.

The Model will enable a country – regardless of its starting point – to identify any gaps in capabilities and commence planning to fill those gaps. Whilst countries will develop their own individual approaches, by doing so within the context of a commonly agreed framework and understanding of capabilities it is hoped that communication and cooperation amongst stakeholders at both national and international levels can be enhanced further.

The WePROTECT Global Strategic Response

The WePROTECT Global Alliance Global Strategic Response (GSR) is a coordinated approach to combating online child sexual exploitation to include greater global insight, an international harmonisation of national approaches, and global solutions over and above the national-led response. The GSR is essentially the companion piece to the Model National Response (MNR); while the MNR is focused on the capabilities required to tackle OCSE at a national level, the GSR is focused on priority areas for international collaboration and capacity-building.

The GSR includes six thematic areas, with associated capabilities required and expected outcomes for each, as well as partners who should work together across borders to deliver them.

Policy and legislation

Developing both the political will to act and legislation to effectively harmonise the approach to criminal offences will result in the renewal of high-level commitment at a national and international level to combat online child sexual exploitation.

Criminal justice

Information sharing, including shared access to international databases through formal data sharing frameworks combined with dedicated, trained officers and prosecutors with expertise in online child sexual exploitation are the best way to identify, pursue and apprehend offenders, including through successful joint investigations and convictions.

Victim impact and services

Effective and timely support for victims, including protection of their identity and giving them a voice, helps to ensure that victims are able to access the support that they need, when they need it.

Technology

The use of technical solutions, including artificial intelligence, to detect, block and prevent harmful material, live streaming and online grooming, which must include wide and consistent adherence among technology sector, will allow those platforms to avoid being used as a tool for online child sexual exploitation.

Societal

There are a number of capabilities that work together within wider society to empower children to protect themselves from online child sexual exploitation, no matter where they live. By ensuring that digital culture development is safer by design (that is, has safety features built-in), and that there is an ethical and consistent approach to media reporting, exposure to illicit content online will be restricted. Meanwhile, education and outreach for children and parents, carers, and professionals, and targeted interventions for offenders, all work to prevent or mitigate the occurrence of online child sexual exploitation.

Research and insight

Finally, threat assessments (such as the Global Threat Assessment 2019), offender research, and work to understand long-term victim trauma will all give government, law enforcement, civil society, academia, and industry a clear understanding of the latest threats.

Appendix 4: Examples of responses to online harms

The examples included here are compiled by the authors and contributors of the ITU policy-maker guidelines.

Educating children against online harms

BBC Own IT App – a wellbeing app aimed at children aged 8-13 receiving their first smartphone. Combining state-of-the-art machine-learning technology to track children's activity on their smartphone with the ability for children to self-report their emotional state, it uses this information to deliver tailored content and interventions to help children stay happy and healthy online.

Featuring specially commissioned content from across the BBC, the app provides useful material and resources to help young people get the most out of their time online and build healthy online behaviours and habits, helping young people and parents have more constructive conversations about their experiences online. The app not collect any personal data or content generated from the user as the entire machine learning runs within the app/within the device of the user.

Project Evolve – Fully resourced digital competency educational framework, identifying the digital skills for each and every age of child to help parents and teachers to understand the competencies that their children should have, together with resources and activities that will provide them with the particular skills.

360 degree safe – An online self-review tool for schools in considering and rating their entire online safety provision providing guidance and support to obtain defined standards.

DQ Institute – Data were collected from 145 426 children and adolescents in 30 countries from 2017-2019 as part of #DQEveryChild, a global digital citizenship movement championed by the DQ Institute, which started in Singapore with the support of Singtel and has quickly expanded in collaboration with the World Economic Forum to include over 100 partner organizations. This movement aimed to empower children with comprehensive digital citizenship competencies from the start of their digital lives using the online education and assessment program DQ World. The data from this movement were used to create the 2020 Child Online Safety Index (COSI). The framework for the COSI assesses and ranks child online safety across 30 countries based on 24 areas grouped into six pillars that affect child online safety.

DQ Pro Family Readiness Package and DQ World provide opportunities for parents to assess their child's digital readiness and, through educational materials, improve digital competencies such as digital citizenship, screen time management, cyberbullying management, cyber security management, digital empathy, digital footprint management, critical thinking, and privacy management.

Australia's eSafety Toolkit for Schools is a suite of resources designed to support schools to create safer online environments. The Toolkit reflects a multifaceted approach to online safety education, and has been categorised into four elements, with resources that:

- prepare schools to assess their readiness to deal with online safety issues and provide suggestions to improve their current practices;
- engage the whole school community to be committed and involved in creating a safe online environment;
- educate by highlighting best practice in online safety education and supporting schools to develop the online safety capabilities of the school community;
- respond to incidents effectively while supporting safety and wellbeing.

The Office of Electronic Communications of Poland-UKE I Click Sensible educational campaign educates children and parents on how to be safer online and how to recognize and manage risk.

ChildFund Viet Nam established the Swipe Safe initiative. This programme educates children on the potential risks online, such as cyber scams, bullying or sexual abuse, and presents advice on methods to stay safe.

Report of the Broadband Commission on *Technology, Broadband and Education: advancing the education for all agenda*, 2013.

Children's Experience Online: Building Global Understanding and Action, UNICEF, 2019.

Global Kids Online research includes a wealth of information about good practice responses to online harms.

Examples of engaging industry

The Australian eSafety Commissioner builds strong partnerships and works with industry to empower all Australians to have safer, more positive experiences online. An example is the eSafety work on safety by design. As part of the initiative, eSafety conducted a detailed consultation process with industry, trade bodies and organisations with responsibility for safeguarding users, as well as parents, carers, and young people. The Safety by Design initiative is designed to encourage and assist industry to ensure user safety is embedded into the design, development and deployment of online services and platforms. eSafety also administers three reporting and complaints schemes: the cyberbullying scheme, the image-based abuse schemes and the online content scheme. eSafety can formally direct certain online service providers to remove content from their services. While the schemes are largely operating as a cooperative model between government and industry, the powers available to eSafety to compel the removal of material provides a critical safety net and drives industry to be proactive in addressing online harms.

The Telia company assumes responsibility to understand and manage the negative impacts of connectivity and to be fully transparent and accountable at the Board level. They also care about Children and young people because they acknowledge they are active users of their services.

The Office of Electronic Communications of Poland-UKE is involving civil society and children in their advocacy campaigns to make them realize what they are signing online.

The Internet Watch Foundation is a partnership organisation that brings together industry, government, law enforcement and NGOs to eliminate child sexual abuse. In 2020, the IWF

had 152 Members across platforms and infrastructure services and offers a Members a range of services to prevent the dissemination of criminal imagery on their platforms.

Legislation coverage

Express political will to prioritize COP by signing the Child Online Safety Universal Declaration (Broadband Commission).

Regulation

Out of the Shadows: shining light on the response to child sexual abuse and exploitation Index (2019) from The Economist Intelligence Unit is the only bench-marking tool that analyses the response of the countries to child sexual abuse and exploitation, including the digital space and the ICT industry response to it.

Identification of abuse of children online

The following are examples of good practice in identifying the abuse of children online.

INHOPE: The INHOPE network was formed in 1999 to combat online CSAM in response to a shared vision of an Internet that is free of child sexual abuse material. In the intervening 20 years, INHOPE has grown to successfully combat the growth, geographical spread, and severity of online CSAM. Today INHOPE hotlines are working on the ground on every continent, receiving reports and rapidly removing CSAM from the Internet, and sharing data with law enforcement.

Microsoft PhotoDNA creates hashes of images and compares them to a database of hashes already identified and confirmed to be CSAM. If it finds a match, the image is blocked. However, this tool does not employ facial recognition technology, nor can it identify a person or object in the image. But, with the invention of PhotoDNA for Video, things have taken a new turn.

PhotoDNA for Video breaks down a video into key frames and essentially creates hashes for those screenshots. In the same way that PhotoDNA can match an image that has been altered to avoid detection, PhotoDNA for Video can find child sexual exploitation content that's been edited or spliced into a video that might otherwise appear harmless.

Microsoft has released a new tool for identifying child predators who groom children for abuse in online chats. **Project Artemis,** developed in collaboration with The Meet Group, Roblox, Kik and Thorn, builds off on Microsoft's patented technology and will be made freely available via Thorn to online service companies that offer a chat function. Project Artemis is a tech tool which helps to raise red flags to the Administrators when any moderation is needed in the chat rooms. This grooming detection technique will be able to detect, address and report predators attempting to lure children for sexual purposes.

Thorn has developed deterrence ads aimed at those searching for child sexual abuse material, which have been served millions of times across four search engines over a period of three years. Additionally, the ads have seen a 3 per cent click-through rate from people seeking help after searching for exploitative material.

Thorn's Safer, a tool that can be deployed directly onto a private company platform to identify, remove, and report CSAM.

Thorn Spotlight, a software that gives law enforcement in all 50 states in the United States of America and in Canada the ability to accelerate victim identification and reduce investigative time by more than 60 per cent.

Geebo, a classified site committed to keeping sexual exploitation off its platform, has never had a case involving child sexual exploitation. They manage to do this in part because of their pre-screening process.

Google AI classifier can be used to detect child sexual abuse material in networks, services, and on platforms. This tool is available for free via the **Google Content Safety API**, which is a toolkit that increases the capacity to review content in a way that requires fewer people to be exposed to it. This tool would help the human experts review material to an even greater scale and keep up with offenders, by targeting imagery that has not previously been marked as illegal material. Sharing this technology would speed up the identification of images.

In 2015, Google expanded their work on hashes by introducing first-of-its-kind fingerprinting and matching technology for videos on **YouTube,** which scan and identify uploaded videos that contain known child sexual abuse material.

During the 2019 Child Safety Hackathon, **Facebook** announced open sourcing of two technologies that detect identical and nearly identical photos and videos. These two algorithms are available in GitHub that allows hash sharing systems to talk to each other, making the systems much more powerful.

The **IWF Hotline** remains perpetually vigilant, not only following up on the thousands of reports from members of the public, who may have stumbled across online child sexual abuse imagery, but also performing a uniquely proactive role of searching for this illegal content on the web. By empowering hotlines to utilise their information and focus resources, more content can be identified and removed. Moreover, IWF is continuously working with Google, Microsoft, and Facebook and other companies within its membership to constantly push technical boundaries. The IWF offers the Reporting Portal solution, that allows internet users in countries and nations without hotlines, to report images and videos of suspected child sexual abuse directly to the IWF through a bespoke online portal page.

The **IWF in collaboration with victim-support charity Marie Collins Foundation** aims to create a new campaign calling on young men to report any self-generated sexual images or videos of children under 18 that they may stumble across while browsing online.

Interpol has created an International Child Sexual Exploitation (ICSE) image and video database, which is an intelligence and investigative tool, allowing specialised investigators from more than 50 countries to share data on cases of child sexual abuse. By analysing the digital, visual and audio content of photographs and videos, victim identification experts can retrieve clues, identify any overlap in cases and combine their efforts to locate victims of child sexual abuse. Currently, the Interpol Child Sexual Exploitation database holds more than 1.5 million images and videos and has helped identify 19 400 victims worldwide.

NetClean ProActive is a software based on signature matching and other detection algorithms that automatically detects child sexual abuse images and videos in enterprise environments.

Griffeye Brain uses artificial intelligence to scan previously unclassified content, compare it with the attributes of known CSAM content and flag suspect items for review by an agent.

RAINN created and operates the National Sexual Assault Hotline in partnership with more than 1 000 local sexual assault report service providers across the country and operates the DoD Safe Helpline for the Department of Defence. RAINN also carries out programmes to prevent sexual violence, help survivors, and ensure that perpetrators are brought to justice.

Safehorizon is a victim assistance non-profit organization that has been standing with victims of violence and abuse in New York City since 1978. Safehorizon offers hotline services to victims of violence.

Project Arachnid is an innovative tool operated by the Canadian Centre, Project Arachnid to combat the growing proliferation of child sexual abuse material (CSAM) on the Internet.

[i] http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf

With the support of:

International
Telecommunication
Union
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-30451-5

Published in Switzerland
Geneva, 2020
Photo credits: Shutterstock