

Guidelines for parents and educators on Child Online Protection 2020



Guidelines for parents and educators 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, the Global Kids Online network, the International Disability Alliance, the International Telecommunications Union (ITU), the London School of Economics and Political Science, Internet matters, Parent Zone International and the UK Safer Internet Centres/SWGfL.

The working group was chaired by Karl Hopwood (Insafe network of Safer Internet Centres (Insafe))¹ and coordinated by Fanny Rotino (ITU).

Invaluable contributions were also received by COFACE-Families Europe, the Australian eSafety Commissioner, the European Commission, the European Council, the e-Worldwide Group (e-WWG), ICMEC, Youth and Media/Berkman Klein Center for Internet and Society at Harvard University as well as individual national governments and private sector stakeholders that share a common objective of making the Internet a better and safer place for children and young people.

These guidelines would not have been possible without the time, enthusiasm and dedication of the contributing authors.

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

- Julia Fossi and Ella Serry (Australian eSafety Commissioner)
- Martin Schmalzried (COFACE-Families Europe)
- Livia Stoica (Council of Europe)
- John Carr (ECPAT International)
- Manuela Marta (European Commission)
- Salma Abbasi (e-WWG)
- Laurie Tasharski (ICMEC)
- Lucy Richardson (International Disability Alliance)
- Carolyn Bunting (Internet matters)
- Fanny Rotino (ITU)
- Sonia Livingstone (London School of Economics & Global Kids Online)
- Cliff Manning and Vicki Shotbolt (Parent Zone International)
- David Wright (UK Safer Internet Centres/SWGfL)
- Sandra Cortesi (Youth and Media)

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

ISBN

978-92-61-30141-5 (Paper version)

978-92-61-30471-3 (Electronic version)

978-92-61-30131-6 (EPUB version)

978-92-61-30481-2 (Mobi version)



Please consider the environment before printing this report.

© ITU 2020

Some rights reserved. This work is licensed to the public through a Creative Commons Attribution-Non-Commercial-Share Alike 3.0 IGO license (CC BY-NC-SA 3.0 IGO).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited. In any use of this work, there should be no suggestion that ITU endorse any specific organization, products or services. The unauthorized use of the ITU names or logos is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: "This translation was not created by the International Telecommunication Union (ITU). ITU is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition". For more information, please visit <https://creativecommons.org/licenses/by-nc-sa/3.0/igo/>

ITU developed its very first set of Child Online Protection Guidelines in 2009. Our aim, back then, was to provide an internationally agreed framework for different stakeholders – parents and educators, industry, policymakers, and children – to keep the youngest Internet users safe, happy and confident online.

Since those early days, the Internet has evolved beyond all recognition. It has become an infinitely richer resource for children, offering educational games, fun activities, and many different ways to share, to learn, and to connect meaningfully to friends, family and the outside world. But at the same time, it has become a much more dangerous place for children to venture unaccompanied.

From issues of privacy, fake news and deep fakes, to violent and inappropriate content, Internet scammers, and the spectre of online grooming and sexual abuse and exploitation, children – and their guardians – face many risks and challenges.

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.

Recognizing this, ITU Member States requested something more than the timely refresh of the COP Guidelines that we have 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 today's children find themselves.

For you, the users of these guidelines, our aim has been to raise awareness of the scope of the challenge, and to provide you with a resource that will help you effectively support young people's interaction with the online world. These guidelines will sensitize you to the potential risks and threats, and help you cultivate a healthy and empowering online environment at home, and in the classroom. They also emphasize the importance of open communication and ongoing dialogue with children, to create a safe space where young users feel empowered to raise concerns.

In addition to reflecting 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.

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, having been co-authored by 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 themselves, as part of a 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. Parents and educators, industry, policymakers – and children themselves – all play a vital role in children's online safety. I hope you will find these guidelines helpful as you accompany the children in your care on an extraordinary voyage to discover the many amazing possibilities the Internet has to offer.

A handwritten signature in black ink, appearing to be 'DBM', written in a cursive style.

Doreen Bogdan-Martin
Director, Telecommunication Development Bureau

Table of Contents

Acknowledgements	iv
Foreword	vii
Executive summary	1
1. Introduction	3
2. What is child online protection?	6
3. Children and young people in a connected world	7
4. Children with vulnerabilities	19
5. New and emerging risks and challenges	22
6. Understanding risks and harms	28
7. The role of parents, carers and guardians can play	33
8. Guidelines for parents, carers and guardians	36
9. The role of educators	43
10. Guidelines for educators	48
11. Conclusion	51
Terminology	52

List of tables and figures

Tables

Table 1: Key areas of consideration for parents, carers and guardians	37
Table 2: Key areas of consideration for educators	48

Figures

Figure 1: Children (%) who play online games at least weekly by gender and age	9
Figure 2: Children (%) who do three or more social activities online at least weekly, by gender	10
Figure 3: Children (%) who do at least one creative activity online at least weekly, by gender and age	11
Figure 4: Children (%) who do three or more information-seeking activities at least weekly, by gender and age	13
Figure 5: Children (%) who have experienced harm online, by gender and age	16
Figure 6: Children (%) who use the Internet at home at least weekly, by gender and age	18
Figure 7: Classification of online risks to children	28
Figure 8: Children stating they have been given any information or advice about how to use the Internet safely, among those who go online at home (2012) or elsewhere (2017, 2018, 2019), by age	44

Executive summary

According to ITU data, there were an estimated 4.1 billion people using the Internet in 2019, reflecting a 5.3 per cent increase compared to 2018 estimates.

Children and young people use the Internet for a variety of purposes, from getting information for a school project to chatting with a friend. They are highly proficient in mastering complex programmes and applications, connecting to the Internet using mobile phones, tablets and other handheld devices such as watches, iPod Touch, e-book readers and gaming consoles.¹

The Internet has also acted as an important tool in the life of the different groups of children and young people with vulnerabilities. For migrant children it maintains a connection with family and friends and offers a window into the culture of their new home. It enables children and young people with disabilities to socialise and to be involved in activities that are unavailable offline, and provides opportunities to be at an equal footing with peers online, with abilities more visible than disabilities.

However, the Internet along with providing access and opportunities also provides risk and harm, with some more prone than others. For instance, for migrant children and young people, the consequences of online breach of confidential information could be dramatic - in the wrong hands, data could be used to identify, and target people based on their ethnicity, immigration status, or other identity signifier²; for children and young people with autism spectrum disorder (ASD), social challenges such as difficulty in understanding others' intentions, can leave this group vulnerable to "friends" with bad intentions; and children and young people with disabilities are more prone to exclusion, stigmatization, and manipulation.

Many parents and guardians are under a common misconception that their child is safer if they use the computer at home, or at school, than elsewhere. This is a dangerous misconception because the Internet can take children and young people virtually anywhere in the world, and in the process, they can be exposed to potentially dangerous risks, just as they could in the physical world. However, children and young people do experience slightly increased risk of harm when accessing the Internet via a smartphone, tablet or other handheld devices. This is because these handheld devices give instant access to the Internet from anywhere and are less likely to be monitored by parents or carers.

These guidelines have been developed within the child online protection (COP) initiative, as part of the ITU Global Cybersecurity Agenda³, with the aim of establishing the foundations for a safe and secure cyberworld not only for today's youth but also for future generations. These guidelines also focus on children with vulnerabilities, particularly, migrant children, children with ASD and children with disabilities.

The guidelines 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 and address issues that might affect all children and young people under the age of 18.

¹ ITU, (2019), Measuring digital development. Facts and figures 2019, <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf>.

² UNICEF (2017), *The State of the World's Children 2017: Children in a Digital World*, <https://www.unicef.org/uzbekistan/media/711/file/SOWC:%20Children%20in%20a%20Digital%20World.pdf>.

³ ITU (2020), *Global Cybersecurity Agenda (GCA)*, <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>.

The UN Convention on the Rights of the Child defines a child as being any person under the age of 18. These guidelines address issues facing all persons under the age of 18 in all parts of the world. However, a young Internet user of seven years of age is very unlikely to have the same needs or interests as a 12-year-old just starting at High School or a 17-year-old on the brink of adulthood. These guidelines have been tailored to give advice or recommendations for different contexts because specific needs require individual consideration and because different local, legal and cultural factors have an important bearing on how these guidelines might be used or interpreted in any given country or region.

1. Introduction

At the global level, one in three Internet users is a under 18⁴, a staggering amount given that in 2018, more than half of the world's population used the Internet. In developing countries, children are leading Internet use, growing up with the Internet, connecting with mobile first.⁵

With more children around the world gaining access, the fulfilment of their rights will increasingly be shaped by what happens online. Internet access is fundamental to the realization of children's rights.

With one child in three being an Internet user, there are still about 346 million children worldwide that are not connected.⁶ Those who could most especially benefit from the opportunities the Internet offers are often are the least connected. We see that in the Africa region around 60 per cent of children are not online, compared to 4 per cent in Europe.⁷

In terms of access to the Internet, there are also significant differences by gender. Research⁸ shows that in every region except the Americas, male Internet users outnumber female users. In many countries, girls do not have the same access opportunities as boys, and even where they do, girls are often monitored and restricted in their Internet use to a much greater extent.

Digital divides go beyond the question of access. Children who rely on mobile phones rather than computers may get only a second-best online experience, and those who lack digital skills or speak minority languages often cannot find relevant content online. Children from rural areas are more likely to experience theft of passwords or money. They also tend to have lower digital skills, spend more time online (especially playing games), and receive less parental mediation and monitoring.⁹

Both children and adults report that the digital divide is an ongoing concern and requires dedicated investment and creative solutions. Children in these settings are coming online in ever greater numbers but many do not benefit from appropriate forms of guidance from parents, teachers, and other significant adults. This continues to place children at risk.

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

⁴ 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>

⁵ ITU (2020), *Measuring the Information Society Report*, https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf.

⁶ UNICEF (2017), *The State of the World's Children 2017: Children in a Digital World*, <https://www.unicef.org/uzbekistan/media/711/file/SOWC:%20Children%20in%20a%20Digital%20World.pdf>.

⁷ UNICEF.

⁸ Araba Sey and Nancy Hafkin (2019), *REPORT OF EQUALS RESEARCH GROUP, LED BY THE UNITED NATIONS UNIVERSITY (United Nations University and EQUALS Global Partnership)*, <https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf>.

⁹ UNICEF (2019). *Growing up in a connected world*. UNICEF Office of Research - Innocenti, Florence, <https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf>.

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

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

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

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

Any approach that deals only or largely with the negative aspects of the technology is very unlikely to be taken seriously by children and young people. Parents and teachers can often find themselves at a disadvantage because young people will very often know more about the technology and its possibilities than older generations. Research has shown that the majority of children are able to distinguish cyberbullying from joking or teasing online, recognising that cyberbullying is designed to harm. In many parts of the world, children indeed have a good understanding of some of the risks they face online¹⁰.

However, while it might be deduced that efforts to skill children to manage online risks are effective, there is still scope to raise the awareness of many more children around the world, particularly among vulnerable groups, and concerted efforts must focus on these children, especially to improve awareness of support services for victims of cyberbullying and other forms of online risks.

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

It is critical that all stakeholders plan for and think through the consequences of these developments for children and find ways to support them to develop the necessary digital literacies not just to survive but to thrive in the digital future. Further investment in the digital skills and literacies of parents and teachers is required to support children to develop the critical thinking and evaluative skills to enable them to navigate fast-paced flows of information of varying quality, and from parents and educators to children, to become digital citizens.¹¹

¹⁰ 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.

¹¹ Council of Europe (2016), *Digital Citizenship Education*, <https://www.coe.int/en/web/digital-citizenship-education/home>.

ITU consultations have demonstrated that some countries struggle to allocate sufficient resources to tackling the digital literacy and safety of children online. However, children report that parents, teachers, technology companies and governments are all important players in developing solutions to support their online safety. An ITU survey of Member States indicates that there is significant support for enhanced knowledge sharing and coordinated efforts to secure the safety of greater numbers of children online.

Balancing children's online opportunities and risks remains a challenge. ITU Member States also indicated that while efforts to promote opportunities for children online must continue to be a priority, this must be carefully balanced with rights to safe conditions under which they can participate in and benefit from the digital world.¹²

¹² ITU News (2018), *Celebrating 10 Years of Child Online Protection*, <https://news.itu.int/celebrating-10-years-child-online-protection/>.

2. 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 establishing a better society. But they can also bring new risks such as exposing them to issues of privacy, illegal content, harassment, cyberbullying, misuse of personal data, grooming and even child sexual abuse.

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

Parents, guardians, and educators also have a responsibility to ensure that children and young people are utilizing Internet sites safely and responsibly.

In recent years, mobile Internet access has increased tremendously and there is no silver bullet solution to protect children and young people online. This is a global issue that requires a global response from all sectors of society, including children and young people themselves.

In order to respond to these growing challenges in the face of rapid development of ICTs, the Child Online Protection (COP) Initiative¹³, a multi-stakeholder international initiative launched by ITU in November 2008, continues to bring partners together from all sectors of the global community to create a safe and empowering online experience for children and young people around the world. It sets out guidelines for all relevant stakeholders including children and young people in all parts of the world on how to keep themselves and others safe online. These guidelines act as a blueprint, which can be adapted and used in a way that is consistent with national or local customs and laws.

This report has been prepared within the COP Initiative by a multi-stakeholder expert working group and aims to provide information, advice and safety tips for parents, guardians and educators on child online protection.

An ITU expert working group co-authored the guidelines in this report, building on the first ITU COP Guidelines, issued in 2009 and updated in 2016. On request of ITU Member States, ITU launched the review process in 2019 that aimed to develop a second version of the guidelines.

These new guidelines include the special situation of children with disabilities when it comes to online risks and harms as well as issues around new technology developments such as the mobile Internet, apps, the Internet of Things, connected toys, online gaming, robotics, machine learning, and artificial intelligence.

¹³ ITU (2020), *Child Online Protection*, <https://www.itu.int/en/cop/Pages/default.aspx>.

3. Children and young people in a connected world¹⁴

At the global level, it has been estimated that one-in-three children is an Internet user and that one-in-three Internet users is a person under 18 years of age.¹⁵ In 2017, half of the world's population used the Internet; among the 15 to 24 age group, the proportion rose to about two-thirds.

"We grew up with the Internet. I mean, the Internet has always been here with us. The grown-ups are like 'Wow the Internet appeared', while it is perfectly normal for us." – Boy, 15 years, Serbia

Among children and young people, the most popular device for accessing the Internet is the mobile phone. This represents a notable shift over the past decade. In Europe and North America, the first generation of Internet users logged on via desktop computer, but the pattern in most developing countries been 'mobile-first' Internet users.

Children and young people prefer using mobile phones because they can carry it around everywhere; they do not have to share it with other household members; it can fulfil several functions at the same time, such as texting, talking, clicking and sharing pictures, and surfing; and it is always on.

"The phone is somehow simpler. We can carry it anywhere, it's smaller and it's easier to work on it. I like it better in this way [using it] by fingers and not with the keyboard." Girl, aged 12 years, Serbia

Surveys have shown that among children and young people who have access to the Internet, girls and boys have similar levels of mobile phone usage to go online. Desktop computers, in comparison, are typically used more by boys.

In practice, most children and young people access the Internet through more than one device and there is tendency of boys to use more devices than girls in every country surveyed.

Children and young people spend on average about two hours a day online during the week and roughly double that each day of the weekend. Some feel permanently connected. But many others still do not have access to the Internet at home – or have only restricted access. However, statistics vary widely and there is a spectrum of views as to how much time children are spending online. Some recent research from the DQ Institute suggests that in Australia children and young people could be spending as much as 38 hours a week online.¹⁶

¹⁴ This chapter is mainly drawn from the following source: UNICEF (2019). *Growing up in a connected world*. UNICEF Office of Research - Innocenti, Florence, <https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf>. The comprehensive research, as part of the comparable high-quality evidence work of the Global Kids Online, collects voices from children in 11 countries, across 4 regions, from 2016 to 2018 (14,733 children aged 9-17 years). The report focuses at the positive effects of ICTs for children and asks at the same time when the use of ICTs becomes problematic in children's lives. All figures of chapter 4 here below are taken from this report. Qualitative and quantitative methodology on which these findings are based can be found at Livingstone, S., Kardefelt Winther, D., and Saeed, M. (2019). *Global Kids Online Comparative Report, Innocenti Research Report*. UNICEF Office of Research - Innocenti, Florence. Online under: <https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html> Further information on the Global Kids Online international research project can be found online under: <http://globalkidsonline.net>.

¹⁵ 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>

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

"I go to a café because we don't have a computer in the house.... We don't have access to the Internet at school." Boy, aged 15-17 years, South Africa

"[I'm connected] All day, but it's not that I use it all day long." Boy, aged 13-14 years, Argentina.

Despite findings from the Global Kids Online (GKO) that similar overall numbers of girls and boys have access to the Internet, however, in some countries, boys have more freedom over Internet usage than girls and that girls are more often monitored and restricted in their Internet use.

A world of fun

Children and young people often go online for a variety of positive and enjoyable reasons. Across the 11 countries surveyed, the most popular activity - for both girls and boys - is watching video clips. More than three quarters of Internet-using children and young people say they watch videos online at least weekly, either alone or with family members.

"When my mother bought the laptop, we started to spend more time together; every weekend we chose a movie and watched it with my grandmother." Girl, aged 15 years, Uruguay.

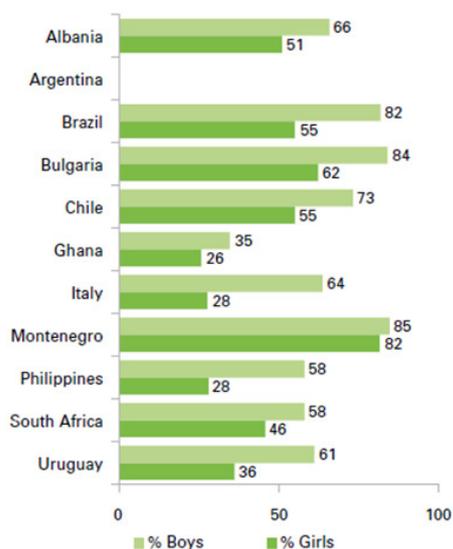
Children and young people also enjoy playing games online, thus exercising their right to play and sometimes their right to learn. Boys are much more likely to play online games in all countries surveyed. Nevertheless, many girls who use the Internet do play online games; for instance, the majority of girls play online games in Bulgaria (60%) and Montenegro (80%). As with watching videos, children and young people are more likely to play online games when they have easier access to the Internet.

"I play online games and make money from them." Boy, aged 17 years, the Philippines.

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

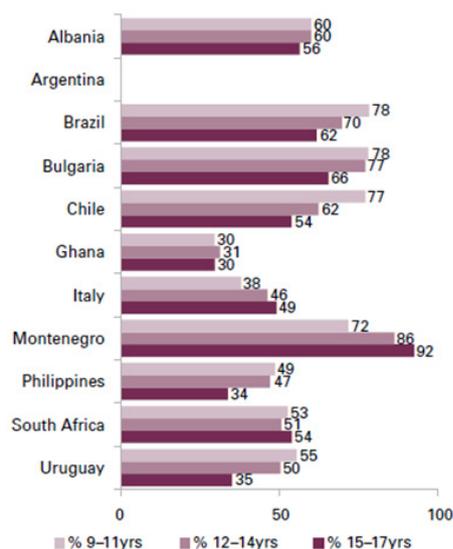
Figure 1: Children (%) who play online games at least weekly by gender and age¹⁷

Figure 20a. Children (%) who play online games at least weekly, by gender



Question C4z-aa: How often have you played online games alone or with other people in the past month? Base: All children who use the internet.

Figure 20b. Children (%) who play online games at least weekly, by age



Question C4z-aa: How often have you played online games alone or with other people in the past month? Base: All children who use the internet.

Source: UNICEF

Making new connections

The Internet, with its instant messaging tools and social networks, has become a crucial meeting point where children and young people can exercise their right to freedom of expression by connecting with their friends and family and with other children and young people who share their interests. In the 11 countries surveyed, many children and young people can be considered 'active socializers', in that they take part in a range of online social activities each week – such as chatting with friends and family, using various messaging tools and networking with people who have similar interests. Some children also report that they find it easier to express their true selves online.

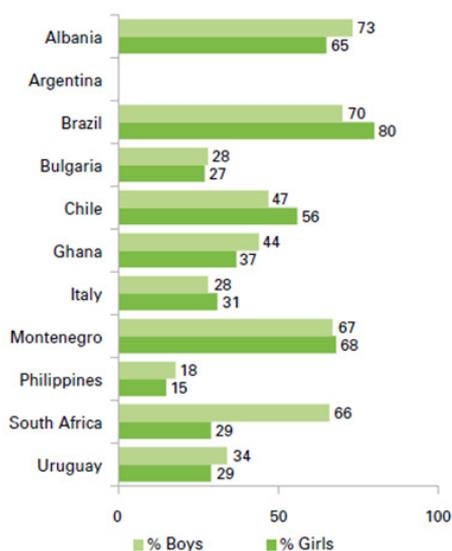
"Online, I can show my true self, there are no rules ... I have more than 5 000 friends online". Boy who identifies as gay, aged 15 years, the Philippines

Online social interactions also increase with age due to various reasons. For instance, some social media websites have a minimum age limit for children and young people, typically gaining more freedom with age.

¹⁷ This figure was taken from: UNICEF (2019). *Growing up in a connected world*. UNICEF Office of Research - Innocenti, Florence, <https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf>

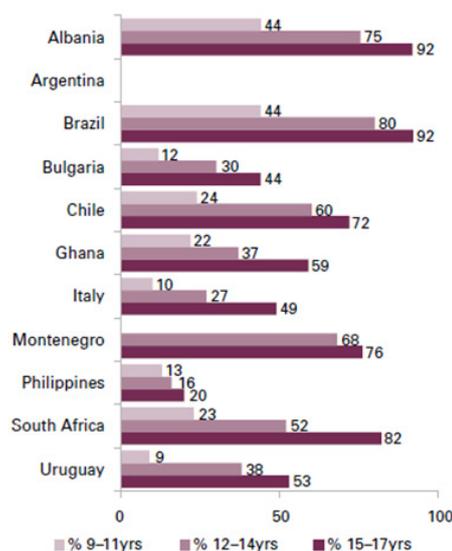
Figure 2: Children (%) who do three or more social activities online at least weekly, by gender¹⁸

Figure 21a. Children (%) who do three or more social activities online at least weekly, by gender



Question C4: How often have you done these social activities online in the past month? Base: All children who use the internet.

Figure 21b. Children (%) who do three or more social activities online at least weekly, by age



Question C4: How often have you done these social activities online in the past month? Base: All children who use the internet.

Note: Children and young people were asked how often they had done the following social activities online in the past month: used the Internet to chat with people from places or backgrounds different to theirs; visited a social networking website; talked to family or friends who lived further away; used instant messaging; participated in a website where people share their interests or hobbies.

Source: UNICEF

It is clear from the above data that the Internet opens up new dimensions for socializing, though parents often complain that children and young people’s online interactions are at the expense of personal contact in the real world.

“In a party, they’re sitting at a table. The 10 of them are each with their little devices.” Parent of adolescents aged 15-17 years, Chile

Such behaviour is not exclusive to children and young people. Some parents make phone calls or browse the Internet during social gatherings – something that bothers many children and young people.

“At the table, when we are eating, and Papa is using his telephone. That is the only time when we are all together, and it really annoys me.” Girl, aged 14 years, Uruguay

With greater access to the Internet, children and young people can widen their horizons, gather information and extend their relationships. With more social interactions, whether online or in-person, they build their experience and skills. GKO research shows that children and young

¹⁸ This figure was taken from: UNICEF (2019). *Growing up in a connected world*. UNICEF Office of Research - Innocenti, Florence, <https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf>,

people who socialize more actively on the Internet are better at managing their online privacy, which helps to keep them safe.

The joy of creation

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

"I have a blog and regularly update it." Girl, aged 15-17 years, the Philippines

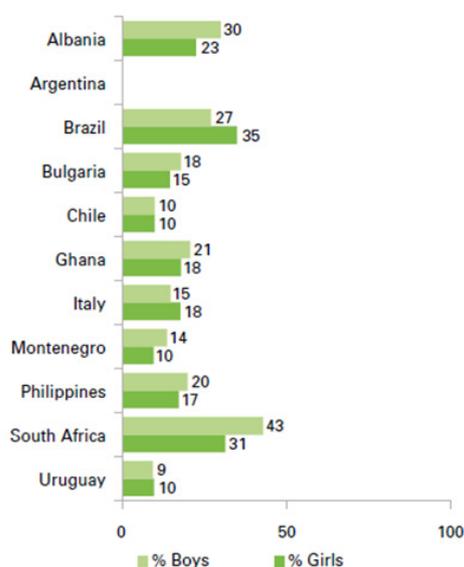
"You can share videos and games. You can share music. You can also share pictures, ideas, games." Girl, aged 9-11 years, Ghana

"I make DIY cards; I post them online. My friends like them." Girl, aged 15-17 years, the Philippines

"Yes, I know how to [hack computers], but do not do it anymore." Boy, aged 15-17 years, the Philippines

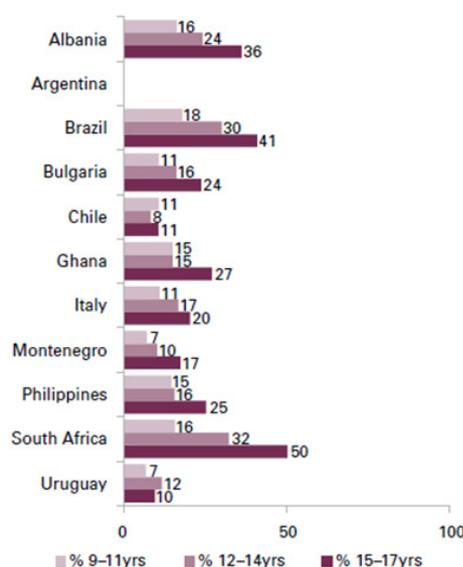
Figure 3: Children (%) who do at least one creative activity online at least weekly, by gender and age¹⁹

Figure 18a. Children (%) who do at least one creative activity at least weekly, by gender



Question C4m-n: How often have you done creative activities online in the past month? Note: In Uruguay, children were not asked about creating blogs online. Base: All children who use the internet.

Figure 18b. Children (%) who do at least one creative activity at least weekly, by age



Question C4m-n: How often have you done creative activities online in the past month? Note: In Uruguay, children were not asked about creating blogs online. Base: All children who use the internet.

¹⁹ This figure was taken from: UNICEF (2019). *Growing up in a connected world*. UNICEF Office of Research - Innocenti, Florence, <https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf>.

Note: Children and young people were asked how often they had done the following creative activities online in the past month: created their own video or music and shared online; created a blog or story or website online; posted videos or music created by someone else.

Source: UNICEF

An appetite for information

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

Many children and young people of all ages use the Internet for homework, or even to catch up after missing classes.

"They asked us to look for names of ministers in Ghana, to search about countries and their currencies. You can get news about other countries." Girl, aged 12-14 years, Ghana

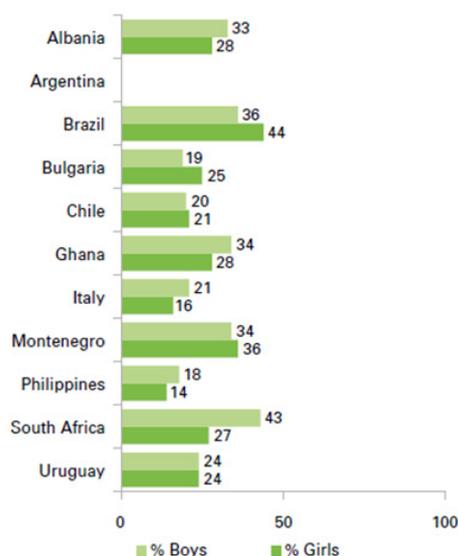
"On the Internet, we can search for all the things we need for school, and we cannot find in the books." Girl, aged 9 years, Serbia

"I failed maths, so I watched a couple of vids [videos] where they explained what I had to study." Boy, aged 15-17 years, Argentina

"If we don't go to school, you can talk to your friend and find out what you missed and stuff. So, it's important to, like, have your friend's WhatsApp." Girl, aged 16-17 years, South Africa

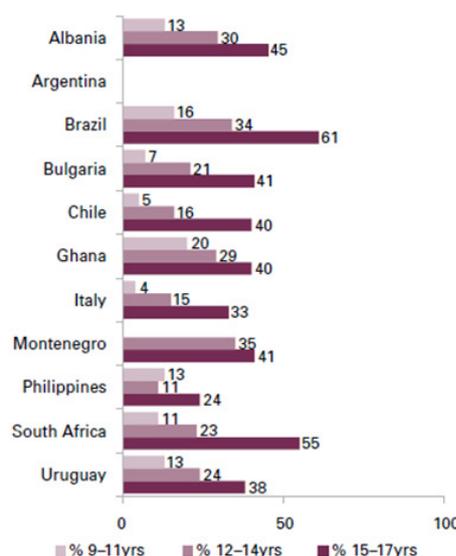
Figure 4: Children (%) who do three or more information-seeking activities at least weekly, by gender and age²⁰

Figure 17a. Children (%) who do three or more information-seeking activities at least weekly, by gender



Question C4: How often have you done information-seeking activities online in the past month? Base: All children who use the internet.

Figure 17b. Children (%) who do three or more information-seeking activities at least weekly, by age



Question C4: How often have you done information-seeking activities online in the past month? Base: All children who use the internet.

Note: Children and young people were asked how often they had done the following information-seeking activities in the past month: learned something new by searching online; looked for information about work or study opportunities; used the Internet for schoolwork; looked for resources or events about their local neighbourhood; looked for the news online; looked for health information for themselves or someone they know. Argentina is omitted due to missing data. Source: UNICEF

Some children and young people are more likely to use the Internet than others to search for information. Data show that the children and young people who use the Internet for a wide range of information-seeking activities tend to be older with the capacity to engage in a broader range of online activities generally and have parents with a supportive and enabling attitude towards their Internet use. This suggests that as children and young people grow older with the right kind of parental support, they tend to gain more online experience and utilise the Internet to their benefit.

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

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

²⁰ This figure was taken from: UNICEF (2019). *Growing up in a connected world*. UNICEF Office of Research - Innocenti, Florence, <https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf>,

The quality and quantity of information that children and young people gather online will depend on their interests and motivation. But what they find will also be affected by the extent of the information available, which will be higher for the most widely spoken languages. Still, minorities can also benefit from information-seeking opportunities – even if they are more limited in number.

“Sometimes, as no one speaks our language in this school, I type something in Romanian into YouTube and hear our voice, and that’s nice, I can understand all.” Roma boy, aged 12 years, Serbia

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

“I watch the foreign news, because I like to see how a country is looking at a situation and how another country is looking at the same situation. Because there are always two sides. For example, America can see something differently and Russia may see something differently.” Girl, 16 years, Serbia

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

“There is so much fake news online.” Boy, aged 15 years, the Philippines

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

Becoming active citizens

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

Young people are most likely to engage politically online.

“Politics ... perhaps she does not look for it specifically. But my daughter, for instance, reads about it on Facebook.” Parent of child aged 13-14 years, Argentina

“But they also give their opinions ... on Twitter ... and that is part of the thing.” Parent of child aged 15-17 years, Argentina

Running risks and suffering harm

Children and young people are exposed to new risks when online, which could lead them to harm. They may come across information on how to self-harm or commit suicide. They can also be confronted with hate speech or material of a violent or sexual nature. The survey conducted by Global Kids Online across countries suggested that the children and young people who engage in a wider range of online activities had experienced more online risks, and perhaps as a consequence of their heightened exposure or their more confident exploration of the Internet.

It is important to remember that risk does not always lead to harm. Children and young people exposed to online risks may not suffer harm if they have the knowledge and resilience to cope with the experience. Therefore, it is important to identify who among them are most vulnerable to online harms and what it takes for risks to be translated into harms to effectively protect children and young people online without unduly limiting their opportunities.

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

In Chile, almost half of adolescents in the 15-17 years age group report something happening online in the past year that had bothered or upset them. When asked to elaborate, they mentioned a wide range of issues, including Internet scams, pornographic pop-up adverts, hurtful behaviour, unpleasant or scary news stories or pictures, discrimination and harassment. In Bulgaria, children and young people are at risk from websites that promote rapid weight loss, which had been viewed by one-quarter of survey respondents.

"There are ugly comments about other people." Girl, aged 13-14 years, South Africa

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

"I was really upset when the guy sent me pornographic pictures." Girl, aged 12-14 years, Ghana.

"I once experienced a stranger asking for 'my price' - meaning how much would it cost to perform a sexual activity." Boy, aged 16 years, the Philippines.

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

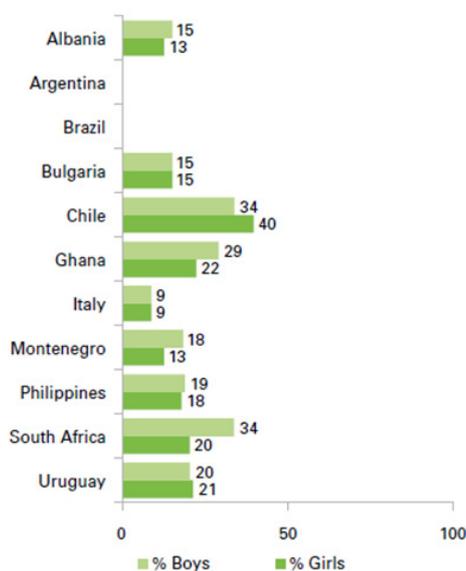
"I was on Instagram and I clicked on a comment and it was so funny, so I wanted to see what other people had to say and I clicked on a link and suddenly naked women popped up." Boy, aged 10 years, Serbia.

"I love horses, everyone knows that. I was searching for some pictures for my wallpaper and stumbled on a gruesome picture of a man cutting a horse." Girl, aged 10 years, Serbia.

"I was very scared ... I saw a picture of a boy who was shot dead." Boy, aged 12-14 years, Ghana.

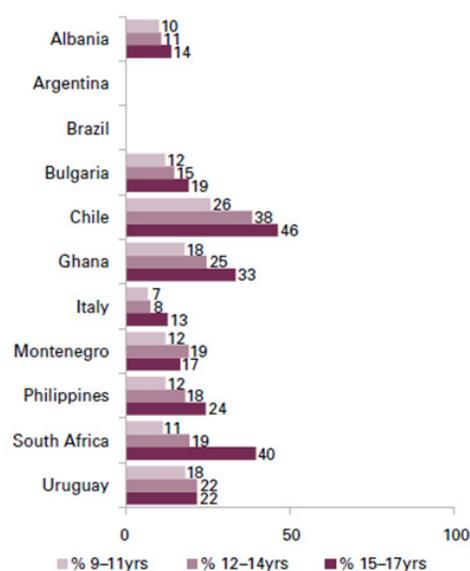
Figure 5: Children (%) who have experienced harm online, by gender and age²¹

Figure 35a. Children (%) who have experienced harm online, by gender



Question F11: In the past year, has anything ever happened online that bothered or upset you in some way (e.g., made you feel uncomfortable, scared or that you shouldn't have seen it)?
Base: All children who use the internet.

Figure 35b. Children (%) who have experienced harm online, by age



Question F11: In the past year, has anything ever happened online that bothered or upset you in some way (e.g., made you feel uncomfortable, scared or that you shouldn't have seen it)?
Base: All children who use the internet.

Source: UNICEF

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

"Everyone started teasing and playing jokes on a boy. He ended up leaving the group." Boy, aged 13-14 years, Argentina.

"I am worried about cyberbullying because it can cause me a lot of emotional damage." Girl, aged 14 years, Uruguay.

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

²¹ This figure was taken from: Global Kids Online (2019). Global Kids Online: Comparative Report, UNICEF Office of Research - Innocenti.

It is worth noting that children and young people do not always recognize 'online' and 'offline' as distinct spaces. For children and young people, online experiences – whether good or bad – are intertwined with the other aspects of their lives.

Privacy is a priority

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

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

"I have one Facebook account for my real friends and another for friends that I just meet online." Girl, aged 14 years, the Philippines.

"When I am connected, I myself am responsible for what I do." Girl, aged 17 years, Uruguay.

More problematically, children and young people online may expose their private information, photographs and communications to potential abuse and inappropriate and unwanted contact.

Children and young people may also make contact with people online who they subsequently meet in person, though this is still relatively rare. Fewer than one-quarter of children and young people across all countries have met someone face to face whom they had first got to know online.

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

Parents sharing content about their children and young people need to consider how this can affect the child. There are concerns that 'sharenting' (parents sharing information and photos of their children online) can violate a child's privacy, lead to bullying, cause embarrassment, or have negative consequences later in life.²² Parents of children with disabilities may share such information in search of support or advice, placing children with disabilities at higher risk for adverse outcomes.

Home is where the Wi-Fi is

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

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

“Adults have a lot of influence over younger people and have to give a good example for them to follow.” Girl, aged 13 years, Uruguay.

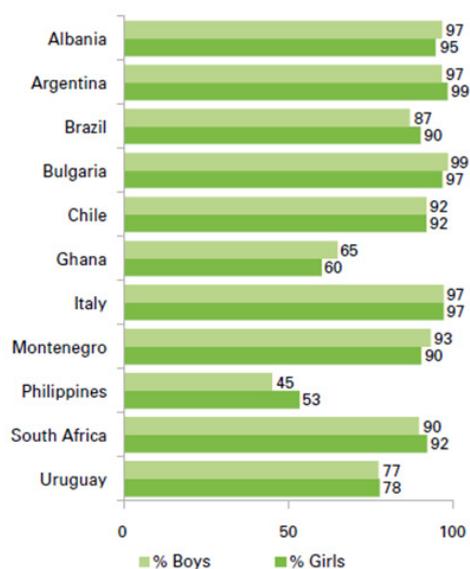
In principle, parents are in a strong position to support children and young people’s Internet use since children and young people primarily access the Internet at home.

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

In most countries, parents are most involved in younger children’s Internet use, helping them to navigate the digital space while at the same time imposing more restrictions on them than on young people. They tend to intervene less as their children grow older, although teenagers would surely still benefit from constructive parental guidance on online opportunities as well as risks.

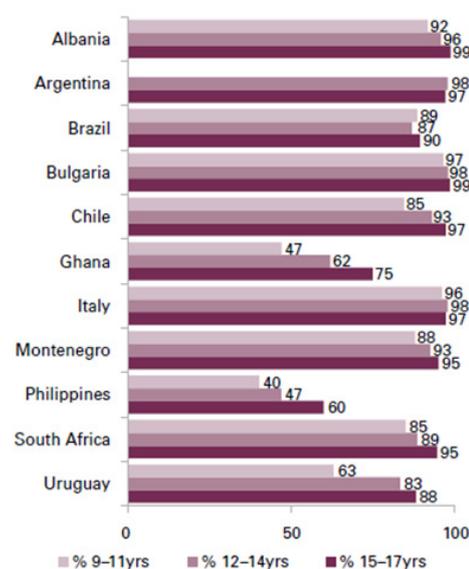
Figure 6: Children (%) who use the Internet at home at least weekly, by gender and age²³

Figure 4a. Children (%) who use the internet at home at least weekly, by gender



Question B6b: Use of internet at home at least weekly.
Base: All children who use the internet.

Figure 4b. Children (%) who use the internet at home at least weekly, by age



Question B6b: Use of internet at home at least weekly.
Base: All children who use the internet.

Source: UNICEF

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

²³ This figure was taken from: Global Kids Online (2019). Global Kids Online: Comparative Report, UNICEF Office of Research - Innocenti.

4. Children with vulnerabilities

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

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

Migrant children

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

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-5²⁶ behaviour diagnostic process.

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

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

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

²⁶ Cardwell C. Nuckols (2013), *The Diagnostic and Statistical Manual of Mental Disorders*, https://dhss.delaware.gov/dsamh/files/si2013_dsm5foraddictionsmhandcriminaljustice.pdf.

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

- The Internet can give children and young people with autism opportunities for socialising and special interests that they may not have offline.
- Social challenges, such as 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

According to some of the first consultative research on children with disabilities' experiences in the digital environment, these children felt that, in many ways, their digital and online lives were very similar to those of children without disabilities. Nevertheless, there were a number of distinct and important differences.²⁷ While considering these, it is important to bear in mind that the challenges and barriers faced by children with disabilities vary significantly, according to the type and nature of impairment. Their particular needs should be considered on an individual basis.²⁸

Children and young people with disabilities face risks online in similar ways to children and young people without disabilities, but they may also face specific risks related to their disabilities. They are 12 per cent more likely to have experienced cyberbullying than children and young people without disability. Some children and young people with disabilities may be less skilled in managing their interpersonal relationships online or distinguishing between true and false information. Some could also be easily manipulated in spending money, sharing inappropriate information, etc. Children and young people with disabilities often face exclusion, stigmatization, and barriers (physical, economic, societal and attitudinal) in participating in their communities. These experiences can have a negative impact on a child with disability seeking out social interactions and friendships in online spaces, which otherwise could be positive, assist in building self-esteem, and create support networks. However, it can also place them at higher risk for incidents of grooming, online solicitation, and/or sexual harassment. Research shows that children and young people experiencing difficulties offline and those affected by psychosocial difficulties are at heightened risk of such incidents.²⁹

Perpetrators of grooming, online solicitation, and/or sexual harassment towards children and young people with disabilities can include not only preferential offenders who target children and young people, but also those who target children and young people with disabilities. Such offenders may include 'devotees' – nondisabled persons sexually attracted to persons with disabilities (most commonly amputees and persons using mobility aids), some of whom even pretend to be disabled themselves.³⁰ Actions by such people may include downloading photos and videos of children and young people with disabilities (that are innocuous in nature),

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

²⁸ *ibid.*

²⁹ Andrew Schrock et al. (2008), *Solicitation, Harassment, and Problematic Content*, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.

³⁰ Richard L Bruno (1997), *Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder, Sexual and Disability*, <https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf>.

and/or sharing them through dedicated forums or social media accounts. Reporting tools on forums and social media often do not have an appropriate pathway to deal with such actions.

Some children and young people with disabilities may face difficulties in using, or even exclusion from online environments due to inaccessible design (e.g. apps that do not allow text size to be increased), denial of requested accommodations (e.g. screen reader software or adaptive computer controls), or the need for appropriate support (e.g. coaching in how to use equipment, one on one support to navigating social interactions).³¹

Some parents of children and young people with disabilities may be overprotective because of their lack of knowledge on how to best guide their child's use of the Internet or protect them from bullying or harassment.³² Some parents of children and young people with disabilities may share information or media (photos, videos) of their child in pursuit of support or advice, placing their child at risk for privacy violations both now and in the future. This also carries the risk of such parents being targeted by uninformed or unscrupulous people offering treatments, therapies, or 'cures' for their child's disability.³³

³¹ UNO (2008), *Convention on the Rights of Persons with Disabilities and Optional Protocol*, <https://www.un.org/disabilities/documents/convention/convoptprot-e.pdf>. For guidelines on these rights, see Article 9 on Accessibility and Article 21 on Freedom of expression and opinion, and access to information

³² Lundy et al. (2019), *TWO CLICKS FORWARD AND ONE CLICK BACK: Report on children with disabilities in the digital environment*, <https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f>.

³³ Sonia Livingstone et al. (2019), *UNICEF Innocenti Research Brief: Is There a Ladder of Children's Online Participation?*, https://www.unicef-irc.org/publications/pdf/IRB_2019-02%2013-2-19.pdf.

5. New and emerging risks and challenges

Internet of Things

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

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

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

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

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

Technical/Privacy problems

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

Social problems

- Exclusion of people.
- Potential for abuse of data.
- Potential for technology to facilitate domestic abuse situations.³⁴

Economic problems

- Job loss.

Environmental problems

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

³⁴ Julie Inman Grant, 2019, 'When "smart" is not necessarily safe: the rise of connected devices extending domestic violence', <https://www.esafety.gov.au/about-us/blog/when-smart-not-necessarily-safe-rise-connected-devices-extending-domestic-violence>.

Connected toys and robotics

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

Opinions on robotics have changed and there has been much debate around the ‘robotification’ of childhood.³⁵ Once seen as dull, dirty and dangerous, industrial and a threat to labour in factory environments, robots have evolved into a tool that are considered to be sophisticated, supportive and social, and something that can be interacted with in homes and in leisure time. While toys have long been fashioned as robots, there have been tremendous changes making the robots more sophisticated. They are no longer just taking the shape and form of the classic science fiction robot, but now coming to life in walking, talking and thinking toys.

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

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

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

Typical features of child-robot interaction include:

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

³⁵ Jochen Peter at the Safer Internet Forum 2017: Better Internet for Kids (2017), Report on the proceedings of the Safer Internet Forum 2017, <https://www.betterinternetforkids.eu/documents/167024/1738388/Report+on+the+proceedings+of+the+Safer+Internet+Forum+2017/fa4db409-4fae-45b1-96ec-35943b7d975d>

While processes reflect:

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

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

Similar concerns also apply to identity development of the child. Research-based studies³⁶ have shown that robots can play an important role in the life of children and young people by helping them to expand and improve their identity search throughout their adolescence. However, robots raise privacy issues, and there is a risk that they may be used as surveillance machines for instance, using them to record anyone within its proximity and hence raising significant safety concerns for both parents and children and young people.

When it comes to relational aspects, relationships with robots might not always reflect real relationships in real life. On the one hand, this might lead to children and young people getting isolated from society, finding comfort in an algorithm that soothes and comforts him or her. However, it could also mean that robots can provide a retreat to “discuss” things that are difficult to bring up in a conversation with parents and peers. Our relationship with robots will always be a servant/master relationship, but robots can increasingly “pretend to feel” and therefore, children and young people might fall into the trap of considering this relationship authentic and mutual.

As Jochen Peter stated, “robots have more to offer than traditional toys but they also present massive risks for the youngest users”.³⁷

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

³⁷ Van Straten, C. L., Peter, J., & Kühne, R. (2019). Child-robot relationship formation: A narrative review of empirical research. *International Journal of Social*

Online Gaming

The gaming industry has surpassed both movie and music in terms of customers and revenue. Moreover, with the advent of mobile gaming which can be accessed on a small mobile device, more people are playing games than ever before. The State of Online Gaming 2019 research highlights that 51.8 per cent are male gamers and 48.2 per cent are female gamers, based on responses from 4 500 consumers in France, Germany, India, Italy, Japan, Singapore, the Republic of Korea, the United Kingdom, and the United States of America, age 18 and older who play video games at least once a week.³⁸ And 21 per cent of video game players are under 18 years of age in United States of America since 2010.³⁹

Recent research in France, Germany, Spain, and the United Kingdom found that 54 per cent of all those aged between 6 and 64 play video games with 77 per cent of them playing for at least an hour a week. Moreover, three quarters of 6 to 15 year-olds in Germany, Spain, Italy, United Kingdom, and France are video game players, these account for over 24 million across five GameTrack European markets. They play a variety of devices but around 7 in 10 gamers play on either consoles or smart devices.⁴⁰

Across the world, there are more than 2.5 billion video gamers. The game PUBG had the highest peak number of players with 3 million players in 1 hour.⁴¹

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

In-game purchases are an increasingly important part of online gaming. With improved Internet connectivity and speed, more players are downloading their games rather than buying a physical copy. In South Africa, online transactions have increased by 13 per cent for gamers from 2018 to 2019.⁴²

Although audiences are diversifying, the games industry is still dominated by male developers and often caters to a presumed heterosexual male audience. Unfortunately, this can often lead to over-sexualised female characters and a distinct lack of non-male, non-white characters to play as.

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

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

³⁸ Limelight Networks (2019), *Market Research: The State of Online Gaming*, http://img03.en25.com/Web/LLNW/%7B02ca9602-173c-43a4-9ee1-b8980c1ea459%7D_SOOG2019_MR_8.5x11.pdf.

³⁹ Statista.com (2019), *U.S. Average Age of Video Gamers in 2019* | Statista, <https://www.statista.com/statistics/189582/age-of-us-video-game-players-since-2010/>.

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

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

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

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

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

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

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

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

There are concerns about online gaming addiction which was defined as *gaming disorder* by the World Health Organisation in 2018.⁴³ This has been defined in the 11th revision of the International Classification of Diseases as a *pattern of gaming behaviour (“digital-gaming” or “video-gaming”) characterized by impaired control over gaming, increasing priority given to gaming over other activities to the extent that gaming takes precedence over other interests and daily activities, and continuation or escalation of gaming despite the occurrence of negative consequences*. It is important to note that in order for gaming disorder to be diagnosed, the behaviour patterns associated with it would need to be seen for at least 12 months.

Another key concern with gaming is the link to online gambling. Some games encourage users to take a chance on loot boxes for example, where a player buys a box using in-game currency (in-game currency is purchased using real money) in order to receive a randomised reward.⁴⁴

Recent research has found that the global loot box market is estimated to be worth £20 billion.⁴⁵

Artificial intelligence and machine learning

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

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

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

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

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

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

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

- Ill-defined problems – problem definition is key to success.
- Data availability – very often, the data is wrong, not appropriate, “dirty”, or not enough. Data used to train and develop AI and algorithmic services are likely to be gained from adult users. This may mean that algorithmic decision-making systems and pattern recognition that use AI may be very adult-centric and therefore result in services that misunderstand/ wrongly categorise risks/behaviour by children. In a similar way, the data sets and models used to shape and inform AI decision-making processes may not accurately represent or consider the needs of some people due to their ethnicity, gender, disability etc. Therefore, children in these underrepresented groups may experience additional, intersectional disadvantage that is further compounded or exploited by AI.
- Neglecting comprehension – sometimes, things work by chance or a model is good, but for something other than the initial problem – for example, there have been stories in the media reporting when AI has mis-identified images in searches.⁴⁶
- The cost of mistakes.

Artificial intelligence is an amazing development, but the conundrum it generates is similar to that of a self-driving car.⁴⁷

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

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

6. Understanding risks and harms

Figure 7 shows a classification of online risks to children. It is acknowledged that there are also health and well-being related risks (excessive use, sleep deprivation etc.).

Figure 7: Classification of online risks to children⁴⁸

Table 3: A classification of online risks to children

	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, & Ólafsson, 2010)

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

Case study 1

This is an example of a boy who watched a video showing the murder of a Jordanian airline pilot by ISIS¹. The boy heard the story and what had happened on the news that was being broadcasted on the radio on his way home from school with his mother. He asked her questions about this, but she wasn't prepared to talk about it. She turned off the radio and they drove home in silence. The boy was really worried about what he had heard - the pilot had been burned alive - and when he got home, he carried out an online search to find out more and try and understand what had happened. One of the things offered to him by the search engine was a video showing what had happened - it was posted by a news channel. The boy said he knew that he should stop watching it as soon as he started but couldn't and he watched the entire video. It had upset him; he was having nightmares and was very distressed by the whole experience - however he hadn't told anyone because he was scared of their reaction and genuinely felt that he would be blamed.

¹ CBS News (2015), *ISIS Video Shows Jordanian Pilot Being Burned to Death*, <https://www.cbsnews.com/video/isis-video-shows-jordanian-pilot-being-burned-to-death/>.

⁴⁸ 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/>

Perhaps the response from the mother is understandable and shows that adults will often struggle to deal with some of the content that can be available online. No matter how challenging and difficult it can be to have these conversations it is important to have them. Parents need to be willing to listen to their children and create an environment where discussion can take place about any issues that are troubling them.

Content

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

Online manipulation

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

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

Contact

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

Online solicitation or grooming

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

⁴⁹ Council of Europe (1957), *Article 23 of the Treaty No. 201: Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, <https://www.coe.int/en/web/conventions/full-list>.

serious harm to the child, for example through production, possession and transmission of child sexual abuse material.⁵⁰

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

Case study 2

This is an example of a 13-year-old girl who was being sent inappropriate pictures from a man on Instagram. The man was sharing naked pictures of himself and had also asked the girl to send naked pictures of herself to him. The girl didn't oblige, she blocked the man, reported him to Instagram and also spoke to some of her friends in case the same thing had happened to them, and it had. Although she had done all of the right things, the girl did not tell her parents for fear of their reaction. She was convinced that they would tell her that she couldn't use Instagram any longer and for her this wasn't an option. She explained that Instagram was where all of her friends shared news, gossip and made their social arrangements, discussed what had happened at school that day and so on. The girl genuinely believed that her parents (in a desire to protect her) would tell her that she had to stop using the platform (Instagram). The problem is that the girl hadn't done anything wrong – the man sending the images was the one who was behaving inappropriately. It is an understandable reaction for parents to want to protect their children but surely it isn't right to penalise your child for something that someone else has done. We should presume that most or all of what this girl was doing on Instagram was absolutely fine. It is important for parents to think about their reaction when their children tell them about a problem that they have encountered online. They also need to listen and provide their support to their children.

Bullying and harassment.

Bullying is bullying wherever and however, it happens. Online bullying can be particularly upsetting and damaging because it tends to spread more widely, with a greater degree of publicity. Moreover, the content circulated electronically can resurface at any time, which makes it harder for the victim of the bullying to get closure over the incident; it may contain damaging visual images or hurtful words; the content is available 24 hours a day. Bullying by electronic means can happen 24/7, so it can invade the victim's privacy even in otherwise 'safe' places such as at home, personal information can be manipulated, visual images altered, and forwarded to others. Further, it can be carried out anonymously.⁵¹

⁵⁰ Committee of the Parties to the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2015), *Opinion on Article 23 of the Lanzarote Convention and its explanatory note*, <http://rm.coe.int/coermpubliccommonsearchservices/displaydctmcontent?documentid=090000168064de98>.

⁵¹ Dr Tanya Byron (2008), *The Report of the Byron Review: Safer Children in a Digital World*, <https://webarchive.nationalarchives.gov.uk/20120107041050/>, <https://www.education.gov.uk/publications/eorderingdownload/dcsf-00334-2008.pdf>.

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

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

Conduct

- Disclosure of personal information leading to the risk of physical harm.
- Physical harm through real-life encounters with online acquaintances, with the possibility of physical and sexual abuse.
- 'Sexting', the sharing of intimate images, that can result in sexual harassment, sextortion, grooming and image-based abuse.⁵⁵

Sexting

A common behaviour by teenagers is 'sexting' (sharing of sexualized images or text via mobile phones). These images and text are often shared between partners in a relationship or with potential partners, but sometimes end up being shared with much wider audiences. It is thought unlikely that young teenagers have an adequate understanding of the implications of these behaviours and the potential risks they entail.⁵⁶

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

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

⁵² Schrock et al. (2008), *Online Threats to Youth: Solicitation, Harassment, and Problematic Content*, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/RAB_Lit_Review_121808_0.pdf

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

⁵⁴ Mueller-Johnson, Eisner and Obsuth (2014), *Sexual Victimization of Youth With a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors*, <http://journals.sagepub.com/doi/10.1177/0886260514534529>

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

⁵⁶ UNICEF (2011), *Child Safety Online: Global Challenges and Strategies*, http://www.unicef.it/allegati/child_safety_online_1.pdf.

- Conduct resulting in health risks such as screen time: Compulsive and excessive use of the Internet and/or online gaming, to the detriment of social and/or outdoor activities important for health, confidence building, social development and general well-being.
- Infringement of their own rights or the rights of others through plagiarism and uploading content (especially photos) without permission. Taking and uploading inappropriate photos without permission has been demonstrated to be harmful to others.
- Infringement of other people's copyright e.g. by downloading music, films or TV programmes that ought to be paid for.
- Misrepresentation of a person's age: either a child pretending to be older to gain access to age inappropriate websites or by an older person pretending to be a child.
- Use of parent's email account without consent: parental consent is required to activate some online accounts, which can be difficult for parents to delete once activated. Children and young people use this method to circumvent permission.

The EU Kids Online 2020 survey illustrates how children and young people are using new media - as opposed to how people think they are using it.⁵⁷ Other research explores how children think that their rights should be protected in the digital environment⁵⁸ as well as work on the experiences of children with disabilities.⁵⁹

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

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

⁵⁷ Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online, <http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf>.

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

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

7. The role of parents, carers and guardians can play

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

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

positive ways. Use in-built tools to review usage patterns around how much time is spent on apps and services.

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

Where to go for help?

Many countries have helplines where children and young people can report a problem. These are widely publicised and different countries have different approaches to getting this message out. It is important that children and young people realise that it is never too late to report a problem and that by doing so they may help others.

While children and young people acknowledge that they sometimes allow themselves to engage in risky behaviour, they do not show a lot of anxiety about the inherent risks of this type of behaviour and show a preference for trying to solve the problems by themselves or within their peer group. This suggests that they turn to their parents or other adults only in cases of potentially 'dramatic' problems. This is a problem particularly with older boys who may be more likely to only use a 'Report Abuse' button⁶⁰ (such as developed by the Virtual Global Task Force) instead of additionally reaching out to parents or other adults. However, this is not the case with all children and young people. We can see that children and young people who are aware of risks, do police their own activities but often do not share a view of the new technologies that implies that adults should be the focal point for judging and monitoring children and young people's behaviour.⁶¹ There is a need to be cautious about making simple distinctions between offline and online worlds, as this, no longer captures how our everyday lives have become, increasingly associated with online technologies. For many children and young people, this means a careful negotiation between the opportunities that technology offers (such as exploring their identity, establishing close relationships and increased sociability) and risks (regarding privacy, misunderstandings and abusive practices) afforded by Internet-mediated communication.⁶²

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

Further information can be found about how to report sexual images of children here:

Internet Watch Foundation – <https://www.iwf.org.uk/>

NCMEC – <https://report.cybertip.org/>

Europol – <https://www.europol.europa.eu/report-a-crime/law-enforcement-reporting-channels-child-sexual-coercion-and-extortion>

⁶⁰ Europol (2019), *2019 Virtual Global Taskforce Releases Environmental Scan*, <https://www.europol.europa.eu/newsroom/news/2019-virtual-global-taskforce-releases-environmental-scan> .

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

⁶² Livingstone (2008), *Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression*, <http://journals.sagepub.com/doi/10.1177/1461444808089415> (last visited 16 January 2020).

8. Guidelines for parents, carers and guardians

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

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

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

Table 1: Key areas of consideration for parents, carers and guardians

Parents, guardians			
	#	Key Areas for consideration	Description
Safety and security of your technology.	1.	Have a discussion with your children. Try to do some online activities with them.	<p>Take an interest in what they are doing online, have a conversation with them. It is important that children and young people don't feel that their parents don't trust them. Filtering, monitoring and restricting access is important but it must happen alongside dialogue and discussion. When children and young people are spending time with others outside the home, they will have access to other (possibly unrestricted) devices, hence, the need for good communication - will they tell you if something went wrong? It is important not to overreact if children and young people tell you about something that has happened online. The important thing is that they have told you and reacting in the right way tend to make them feel confident that you can help them, and they will come back in the future.</p> <p>It can be helpful for children and young people to have an understanding as to what the Internet is, so that they have a better awareness of the Internet "space" in which their favourite platforms such as Instagram, Snapchat or YouTube exist. The Internet can often seem like an abstract place for children and young people and without some understanding of it, they can find it harder to frame the risks and recognise/visualise them. A possible analogy could be that of a large city which has lots of nice places and lovely people but also areas that you wouldn't visit as they could be risky. This will help children and young people to reflect on different "audiences" that they might encounter when they are online and how information can flow etc.</p> <p>Parents should take an interest in what their children do online and be prepared to share digital experiences with them as a way to foster trust and open up dialogue.</p>

Parents, guardians		
#	Key areas for consideration	Description
2.	Identify the technology, devices and services across your family / household.	<p>Starting with devices, identify all the devices in your home that are connected, including mobile phones, laptops, tablets as well as smart televisions, gaming consoles, fitness trackers in use across the family.</p> <p>Identify the online services and apps that are being used across the family across all these devices.</p>
3.	<p>Install firewall and antivirus software on all devices.</p> <p>Consider whether filtering and blocking or monitoring programmes can help support and are suitable for your family.</p>	<p>Ensure that your devices have antivirus and malware protection installed and that it is kept up to date. Teach your children the basics of Internet security. E.g. is your operating system up to date, are you using the latest version of an app? Are the latest security patches installed?</p> <p>Filtering and monitoring products are useful - but issues of trust and privacy should also be considered. Parents should have a conversation with their children about why they are using such products in order to keep the family safe.</p>
Rules	<p>4. Agree expectations as a family about using the Internet and personal devices, giving particular attention to issues of privacy, age inappropriate websites, apps and games, bullying, screentime and stranger danger.</p> <p>Also ensure that there is a culture of support in the home so that children and young people feel able to seek support from parents/carers.</p>	<p>As soon as children and young people begin to use technology, discuss and establish a list of agreed rules. These rules should include when children and young people can use the Internet and how they should use it, as well as expectations of screen time.</p> <p>Digital Role Model - It is important that parents set the right example for their children. They are more likely to adopt the correct behaviours if these are being modelled by parents/carers.</p> <p>This might be extended to taking and sharing photos - consent should be sought before posting any images online. Consideration of parents' own use of the Internet and social media in relation to their child, such as sharing personal stories or photos about the child. Consider the child's privacy both now and for the future.</p> <p>Children and young people need to be able to come and talk about whatever online (and offline) pressures and challenges that they are facing. One way of enabling discussion is to use opportunities where stories about the Internet/online behaviour feature in the media. This will de-personalise the issue but will allow to children and young people to express an opinion.</p>

Parents, guardians			
	#	Key areas for consideration	Description
Parents' and Guardians' education	5.	Be aware of the online and mobile services used by your children (i.e. social media, websites, apps, games etc.) and have a good understanding of how children spend their time online	<p>Have some understanding of how to ensure that children and young people are using apps and platforms as safely as possible, including making accounts private, being aware of age restrictions etc.</p> <p>Make use of the tools which come with mobile devices such as Family Link or other parental control tools. Check to see if any products are sold or in-app purchases are included.</p> <p>Try to have some understanding of the motivations of children and young people when they are online. Why are they using particular websites and services? What do different websites and services mean in terms of friendship groups, sense of identity, and belonging? This understanding will also you to better understand the social and emotional challenges children and young people may face, (which can sometimes result in risky behaviour).and give them insights into how to build resilience.</p>
Internet sites features review	6.	Consider age of digital consent	<p>Some countries have laws specifying a minimum age at which a company or website can ask a young person to provide personal information about themselves without first obtaining verifiable parental consent. This age of 'digital consent' typically ranges between 13 and 16. In some countries it is considered to be good practice to require parental consent before asking younger persons for their personal data while in others, it is enshrined in law (see the GDPR article 8 for EU member states). Many websites which cater for younger children will ask for parental consent before allowing a new user to join. Check each service for minimum age requirements.</p>

Parents, guardians		
#	Key areas for consideration	Description
7.	Control use of credit cards and other payment mechanisms	Many devices, apps and services can be used to make purchases and carefully manage access to parental accounts with stored payment mechanisms and credit cards. It is important to keep your credit and debit cards secure, and do not disclose your pin numbers in order to prevent unauthorised access.
8.	Reporting	Know how to report problems on the platforms that your children are using and how to delete or make changes to profiles - as children get older, ensure that they know how to do this. Also be aware of local reporting helplines.
9.	Advertising, misinformation and disinformation	Be aware that advertising can be inappropriate or misleading. Talk to your children about how they can report ads and take more control over what they see online. It is important to recognise that what children and young people see online can influence their views. Engage with them to help them to develop their online media literacy.

Parents and guardians			
	#	Key areas for consideration	Description
Children's education	10.	Create a culture of support	<p>Children and young people need to understand that the online world is a reflection of the offline world - with good and bad experiences. It is important that children and young people feel confident that they can ask you for help and support if something has gone wrong as well to be able to provide support for others online.</p> <p>Depending on the age of your children, it may be helpful to understand the content they have posted and any online profile.</p> <p>Children and young people need to be able to recognise online risks -some are obvious but others less so - such as coercion, blackmail, shaming. These mechanisms are all used by perpetrators and criminals.</p> <p>Children and young people also need to understand that online access comes with responsibility. They need to know that laws apply both online and offline and that they should behave in the right way.</p>
	11.	As children and young people learn more about the online world, they may wish to meet up with people they don't know in real life, but who they've formed a relationship with online. It's important you take the right steps to educate them on the dangers of meeting up with a stranger they've been speaking with online.	<p>Children and young people could be in real danger if they meet in person strangers with whom they have communicated only online. People online may not be who they say they are. However, if a strong online friendship does develop and your child wishes to arrange a meeting, rather than risk them going alone or unescorted, make it clear that you would rather go with them, or ensure another trusted adult goes. Clearly this will depend upon the age of the child.</p> <p>It is also important to be aware that there has been an increase in non-contact offending with criminals and perpetrators seeking not to meet a child, but to get sexually explicit content from them.</p>
	12.	The importance of personal information.	<p>Help your children understand and manage their personal information. Explain that children and young people should post only information that you - and they - are comfortable with others seeing. They should not be sharing personally identifiable information. Remind children and young people that they have an online reputation which needs to be managed. Once content has been shared it can be difficult to change/adapt.</p>

Parents and guardians			
	#	Key areas for consideration	Description
Children's education	13.	Ensure children and young people understand what it means to post photographs on the Internet, including photos of themselves and their friends	Explain to your children that photographs can reveal a lot of personal information. Children and young people should understand the risks of using cameras and uploading content. Ideally images of others should not be uploaded without their consent. This should include parents taking and uploading images of their children. Equally, it is important that children and young people understand that sometimes it may be others, in their friend and family network who could let out information, so they should speak to their friends and families as well educate them about oversharing. Encourage your children not to post photographs of themselves or their friends with clearly identifiable details such as street signs, license plates on cars, or the name of their school on their sweatshirts.

9. The role of educators

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

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

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

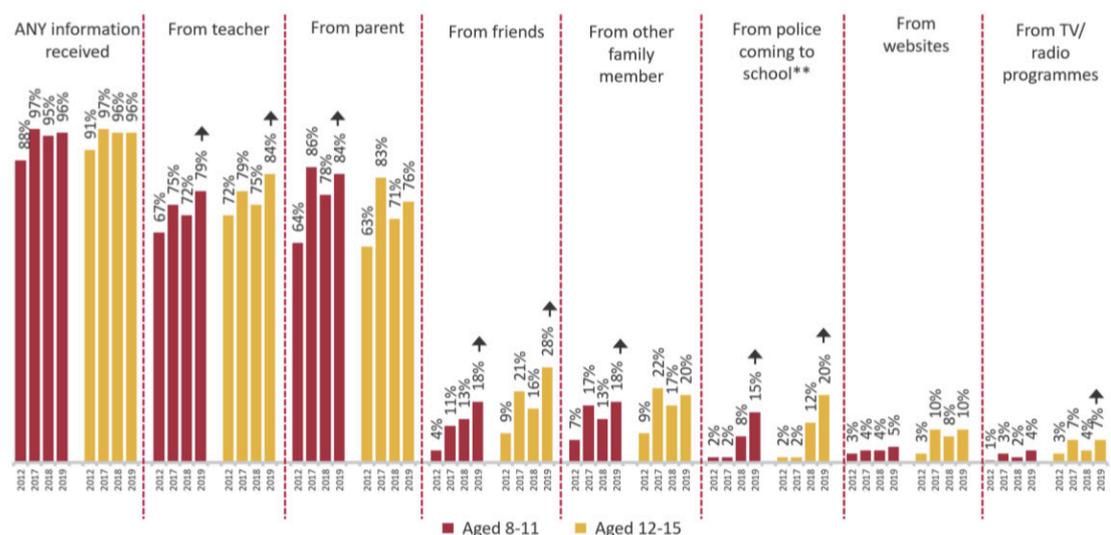
Educators can help children and young people use technology wisely and safely:

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

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

- Having a single point of contact in the school and being able to collect and record online safety incidents which will give the school a better picture of any issues or trends which need to be addressed.
- Ensuring that the management team and school governors have an adequate awareness of online safety in the school.
- Having a regular audit of all online safety measures.
- Appreciating the educational and psychological effects that the Internet and online technologies can have on children and young people.
- Children and young people’s use of Internet technology has risen dramatically in recent years and has been accompanied by a growing concern about issues of online safety. Historically, there has been a recurring moral panic about the potential danger of communication technologies, and this has particularly been the case for young women. However, it has been argued that when such dangers are actually investigated, it appears that very often it is not the technology as such that is the culprit but more the increase in activity of the children and young people using the technology, more the anxieties about loss of parental control. Educators have been perceived to have a vital role in promoting and ensuring Internet safety. Parents across the world appear to believe that schools should have a central role in educating children and young people in the safe use of technology, but it is also clear from research that the main source of information on online issues for children and young people is from school and from parents.⁶⁴ Further guidance on competencies that should be included in this type of education were identified as part of the Council of Europe Digital citizenship education project.⁶⁵

Figure 8: Children stating they have been given any information or advice about how to use the Internet safely, among those who go online at home (2012) or elsewhere (2017, 2018, 2019), by age⁶⁶



Source: Ofcom

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

⁶⁵ Council of Europe (2018), *Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers, Building a Europe for and with Children*, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>.

⁶⁶ Ofcom (2020), Children and Parents: Media Use and Attitudes Report 2019, https://www.ofcom.org.uk/_data/assets/pdf_file/0024/190518/children-media-use-attitudes-2019-chart-pack.pdf.

- Early approaches to online safety focused largely on technological solutions, such as the use of filtering software, but in recent years, there has been an increasing mobility of information technology and as a result, more traditional desktop computers are no longer the sole access point to the Internet. Increasing numbers of mobile phones, tablets, personal digital assistants and gaming consoles offer broadband connections and children and young people can access the Internet while at school, at home, in the library, at an Internet café, a fast-food outlet, a youth club or even travelling to school on public transport. Schools offer the opportunity to work on the Internet, collaboratively within a closed network or simply surrounded by other children and young people. Obvious initial measures include setting up effective security in the network. Children and young people may have personal devices that are not covered by network protection and this is why education, discussion and dialogue are crucial.
- Online safety policies need to be designed and implemented to involve a wide range of interest groups and stakeholders. These include:
 - head teachers;
 - governors;
 - senior management;
 - classroom teachers;
 - support staff;
 - parents or caregivers;
 - local authority personnel;
 - where possible, Internet service providers and those who are providing Internet and broadband services to schools.

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

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

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

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

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

The problems that arise in relation to new technologies do not apply to all children and young people, and when problems do arise, they depend on the age of the children and young people using these technologies. At the end of 2008, the Internet Safety Technical Taskforce in the United States of America produced a report on enhancing child safety and online technologies which provided a useful literature review of original, published research addressing online sexual solicitation, online harassment and bullying, and exposure to problematic content.⁶⁷ Within this report it was noted that, "There is some concern that the mainstream media amplifies these fears, rendering them disproportionate to the risks youth face." Over ten years later and this is still the case with parents and educators being bombarded with attention grabbing headlines that are more likely to encourage adults to restrict access to online services than educate and empower children to use them safely.

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

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

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

A useful way to classify online risks to children was presented in Figure 7.

Informal education settings

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

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

Managing devices, filtering, and communication

Support staff, volunteers, and children may be more likely to access services via their own devices in informal settings or systems to manage devices, and filtered content may be less

⁶⁷ ISTTF (2008), *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

available or less robust than in schools. Therefore, ensuring that practitioners and children understand how to secure and manage their own device may require a greater focus in informal settings. Equally with less sophisticated filtering options available, educators and children should not overly rely on them for protection.

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

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

Training and support

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

Table 2 identifies some of the key areas of consideration for educators.

10. Guidelines for educators

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

Table 2: Key areas of consideration for educators

	#	Key areas for consideration	Description
Safety and security of devices	1	Ensure that all devices are secure and password protected.	Teachers are as vulnerable as anyone else to cyber-attacks, malware, viruses and hacks. It is important that teachers should ensure that any device that they are using is properly protected (with strong passwords) and locked when not in use. (e.g. if a teacher needs to leave the classroom, then any device that they are using should be locked or the teacher should logoff/sign out).
	2	Install anti-virus software and firewalls.	Ensure that all devices have a firewall and anti-virus software installed and that this is kept up to date.
Policies	3	All schools should have a policy which governs where and how technology can be used within the school by different stakeholders and how child protection incidents are managed - including online.	Teachers need to ensure that they follow the policy regarding the use of mobile technology and other electronic devices. It is important that teachers model the correct behaviour when using devices. Schools should specify where and when mobile devices can be used.
	4	Images of pupils.	Schools should have a policy which details whether photos of pupils can be taken. Are staff able to take photos for educational purposes? Has the relevant permission been granted by parents/carers/pupils themselves? Ideally the policy should state that personal devices should not be used for this purpose in order to safeguard both pupils and staff.

	#	Key areas for consideration	Description
Filtering and monitoring	5	Ensure that the Internet feed provided by the school is both filtered and monitored.	<p>Pupils should not be able to access harmful or inappropriate content from the school IT systems. No filtering system can ever be 100 per cent effective and it is important to support these technical solutions with good teaching and learning as well as effective supervision. As a minimum the filtering should prevent access to illegal content as well as content deemed to be inappropriate or harmful. As an example, the following categories of harmful content should be considered:</p> <ul style="list-style-type: none">• Discrimination• Hate speech• Drug or substance abuse• Extremism• Pornography• Piracy and copyright theft• Self-harm or suicide content• Extreme violence

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

11. Conclusion

Information and communication technologies (ICTs) have transformed modern lifestyles. They have provided us with real-time communications, borderless and almost unlimited access to information and a wide range of innovative services. At the same time, they have also created new opportunities for exploitation and abuse. Without proper safeguards, children and young people - among the heaviest users of the Internet - are at risk of unwanted sexual solicitations, harassment, and unwanted exposure to violent, sexual and other distressing material.

Without proper mechanisms to create a safe cyber environment, children and young people will remain vulnerable. Although there is increasing awareness of the risks related to the insecure use of ICTs, there is still a significant amount of work to do. It is, therefore, crucial that parents and educators discuss and decide with children and young people what is appropriate and safe for their use, as well as how to behave responsibly using ICTs.

In working together, parents, educators, children and young people can reap the benefits of ICTs, while at the same time minimizing the possible dangers for children and young people.

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, 2016⁶⁸ (Luxembourg Guidelines), by the Council of Europe Convention: Protection of Children against Sexual Exploitation and Sexual Abuse, 2012⁶⁹ as well as by the Report Global Kids Online, 2019⁷⁰.

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 are considered adults, unless majority is attained earlier under national law.⁷¹

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).⁷²

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.⁷³

Alexa

Amazon Alexa, known simply as **Alexa**, is a virtual assistant AI developed by Amazon. is capable of voice interaction, music playback, making to-do lists, setting alarms, streaming podcasts, playing audiobooks, and providing weather, traffic, sports, and other real-time information, such as news. Alexa can also control several smart devices using itself as a home automation system. Users are able to extend the Alexa capabilities by installing "skills" (additional functionality developed by third-party vendors, in other settings more commonly called apps such as weather programs and audio features).⁷⁴

⁶⁸ Terminology and Semantics (2016), *Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>.

⁶⁹ Council of Europe (2012), *Protection of Children against Sexual Exploitation and Sexual Abuse: Council of Europe Convention*, https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf.

⁷⁰ Globalkidsonline.net (2019), *Done Right, Internet Use Can Increase Learning and Skills*, <http://globalkidsonline.net/synthesis-report-2019/>.

⁷¹ UNICEF and ITU (2015), *Guidelines for Industry on Child Online Protection*, https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

⁷² Council of Europe (2020), *What's AI?*, <https://www.coe.int/en/web/artificial-intelligence/what-is-ai>.

⁷³ OECD (2019), *Recommendation of the Council on Artificial Intelligence*, <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>.

⁷⁴ Amazon (2019), *Alexa Skills Kit Official Site: Build Skills for Voice*, <https://developer.amazon.com/en-US/alexa/alexa-skills-kit>.

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.⁷⁵

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.⁷⁶

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 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."⁷⁷ Sexual exploitation and abuse of children increasingly take place through the Internet, or with some connection to the online environment.⁷⁸

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.⁷⁹ 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.⁸⁰ 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

⁷⁵ OHCHR (1990), *Convention on the Rights of the Child*, <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>.

⁷⁶ UNICEF and ITU (2015), *Guidelines for Industry on Child Online Protection*, https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf

⁷⁷ Terminology and Semantics (2016), *Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>.

⁷⁸ Terminology and Semantics (2016), *Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>.

⁷⁹ Terminology and Semantics (2016), *Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>.; UNICEF and Global Kids Online (2019), *Global Kids Online Comparative Report*, <https://www.unicef-irc.org/publications/pdf/GKO%20LAYOUT%20MAIN%20REPORT.pdf>.

⁸⁰ WePROTECT Global Alliance (2016), *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response.*, <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf>; Broadband Commission (2019), *Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online*, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

'child pornography' risks insinuating that the acts are carried out with the consent of the child, and represent legitimate sexual material".⁸¹

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.

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.⁸²

Cyberbullying, also referred to as Online bullying

Cyberbullying describes 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.⁸³ 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"⁸⁴. 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).

⁸¹ Terminology and Semantics (2016), *Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>

⁸² Jeremy Greenberg (2017), *Dangerous Games: Connected Toys, COPPA, and Bad Security*, <https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/>.

⁸³ Anna Costanza Baldry, Anna Sorrentino, and David P. Farrington (2019), *Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities*, <https://doi.org/10.1016/j.childyouth.2018.11.0058>.

⁸⁴ Terminology and Semantics (2016), *Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf> ; "UNICEF and Global Kids Online (2019), *Global Kids Online Comparative Report*, <https://www.unicef-irc.org/publications/pdf/GKO%20LAYOUT%20MAIN%20REPORT.pdf>

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”⁸⁵.

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.⁸⁶

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.⁸⁷ 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.⁸⁸

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.

Governors

Describes all person who have held a position in the school management/ governance structure.

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

⁸⁵ UNICEF and Global Kids Online (2019), *Global Kids Online Comparative Report*, <https://www.unicef-irc.org/publications/pdf/GKO%20LAYOUT%20MAIN%20REPORT.pdf>.

⁸⁶ Council of Europe (date?), *Digital Citizenship and Digital Citizenship Education*, <https://www.coe.int/en/web/digital-citizenship-education/home>.

⁸⁷ Western Sydney University-Claire Urbach (date?), *What Is Digital Literacy?*, https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy.

⁸⁸ Dr. Andrew K. Przybylski, et al. (2014), *A Shared Responsibility. Building Children’s’ Online Resilience Report*, <https://parentzone.org.uk/sites/default/files/Building%20Online%20Resilience%20Report.pdf>.

Internet or other digital technologies to facilitate either online or online sexual contact with that person persuading the child to have a sexual relationship.⁸⁹ 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.⁹⁰ It further includes services such as radio as well as among others broadband, network hardware and satellite systems.

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.⁹¹

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.⁹²

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

⁸⁹ Terminology and Semantics (2016), *Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>

⁹⁰ UNICEF and ITU (2015), *Guidelines for Industry on Child Online Protection*, https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

⁹¹ UNICEF (2019), *Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry*, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

⁹² UNICEF and ITU (2015), *Guidelines for Industry on Child Online Protection*, https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

educators) who has a legal responsibility for a child. Parental responsibility will vary from country to country as will legal parental rights.

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.⁹³

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.⁹⁴ 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 “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)”.⁹⁵

The Internet of Things

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.⁹⁶

⁹³ US Federal Trade Commission (1998), *Children’s Online Privacy Protection Act*, <https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5>.

⁹⁴ Terminology and Semantics (2016), *Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>

⁹⁵ Terminology and Semantics (2016), *Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, <http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>

⁹⁶ Ntantko (2013), *The Internet of Things, Digital Single Market*, <https://ec.europa.eu/digital-single-market/en/internet-of-things>.

URL

The abbreviation stands for 'uniform resource locator', the address of an Internet page.⁹⁷

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.⁹⁸

WI-FI

Wi-Fi (Wireless Fidelity) is the group of technical standards that enable data transmission over wireless networks.⁹⁹

⁹⁷ UNICEF and ITU (2015), *Guidelines for Industry on Child Online Protection*, https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

⁹⁸ NASA (date?), *Virtual Reality*, online under: <https://www.nasa.gov/Software/VWT/vr.html>.

⁹⁹ US Federal Trade Commission (1998), *Children's Online Privacy Protection Act*, <https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5>.

With the support of:



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

ISBN: 978-92-61-30471-3



9 789261 304713

Published in Switzerland
Geneva, 2020
Photo credits: Shutterstock