Guidelines for Industry on Child Online Protection

2014 edition

ITU unicef

www.itu.int/cop

ACKNOWLEDGEMENTS

This publication was developed through a consultative process led by the International Telecommunication Union (ITU) and UNICEF and benefited from the expertise of a wide range of contributors from leading institutions active in the information and communications technologies (ICT) sector and on child online safety issues.
UNICEF Corporate Social Responsibility Unit: Amaya Gorostiaga, Eija Hietavuo
UNICEF Child Protection Section: Clara Sommarin
The document also benefited from the review of the following UNICEF colleagues:
Christian Salazar, Maniza Zaman, Bo Viktor Nylund, Susan Bissell, Kerry Neal, Joost Kooijmans and Julia Schulteis.
ITU: Carla Licciardello, Preetam Maloor, Marco Obiso, Despoina Sareidaki
Editor: Catherine Rutgers
ITU and UNICEF are grateful to Jenny Jones, GSMA and John Carr, Children's Charities' Coalition on Internet Safety, for their continuous support and invaluable guidance to the overall process.
Moreover, we acknowledge the precious work of our COP Partners, especially (listed in alphabetical order):

- Anika Holterhof and Steven Malby, United Nations Office on Drugs and Crime (UNODC)
- Anjan Bose, ECPAT International
- Ellen Blackler, The Walt Disney Company
- Francesca Bosco, United Nations Interregional Crime and Justice Research Institute (UNICRI)
- Julian Coles (BBC) and Giacomo Mazzone, European Broadcasting Union (EBU)
- Kim Sanchez, Microsoft Corporation
- Martin Schmalzried, Confederation of Family Organizations in the European Union (COFACE)
- Myla Pilao, Trend Micro
- Paul Cording, Vodafone Group
- Robert Shilling and Mick Moran, Interpol
- Roberto Masotti, Emanuela Negro, and Lara Campodonico, Telecom Italia
- Sandra Marchenko, International Centre for Missing and Exploited Children (ICMEC)
- Susie Hargreaves and Fred Langford, Internet Watch Foundation (IWF)

Finally, ITU and UNICEF thank the wide range of stakeholders who contributed to the development of the content during the open consultation held in December 2013.

Contents

Glossary

ADOLESCENT

UNICEF (and other United Nations agencies) define adolescents as 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 those 18–19 years old are considered adults, unless majority is attained earlier under national law.

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.

CHILD RIGHTS IMPACTS

Companies can impact the rights of children, either positively or negatively, through the ways in which they operate their facilities; develop, deliver and market products; provide services; apply leverage through business relationships with key stakeholders and partners; and exert influence on economic and social development. Under the United Nations Guiding Principles on Business and Human Rights, companies have a responsibility to identify, prevent, mitigate and, where appropriate, remediate their potential or actual negative impacts on human rights.

Recognizing the need for explicit guidance about what it means for business to respect and support children's rights, the United Nations Global Compact, Save the Children and UNICEF – together with companies and other stakeholders – released the Children's Rights and Business Principles in March 2012. The Principles call on companies to respect children's rights, avoid any infringement on the rights of children, and address any adverse child rights impact with which the business is involved. The Principles also encourage companies to support children's rights by taking voluntary actions that seek to advance children's rights through core business operations, products and services, strategic social investments, advocacy, public policy engagement, and working in partnership and other collective action. To access the full set of Children's Rights and Business Principles, see www.unicef.org/csr/12.htm.

CHILD SEXUAL ABUSE MATERIAL

Child sexual abuse material refers to any material that visually depicts a child in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes, including photography, video, drawings, cartoons, text and live streaming.[1] Although the term 'child pornography' is used commonly in legislation and international conventions, this term is not used in the Guidelines for Industry on Child Online Protection because 'pornography' is frequently understood to be associated with depictions of sexual activity between consenting adults. For this reason, use of the term 'child pornography' can mischaracterize sexual representations where children are involved, since it does not highlight the abusive/exploitative aspects of this phenomenon or reflect the wide spectrum of child sexual abuse materials, and its use can therefore cause misunderstanding.

CYBERBULLYING

International law does not define cyberbullying. For the purpose of this docu-

1. The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

ment is it defined as wilful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices. It may involve direct (such as chat or text messaging), semipublic (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).[2]

GROOMING

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'.[3]

INTERNET AND ASSOCIATED TECHNOLOGIES

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

NOTICE AND TAKEDOWN

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

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.

URL

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

WI-FI

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

BROADCASTING SERVICES

Please refer to the online glossary on www.itu.int/cop.

2. Schrock, A., and D. Boyd, 'Online Threats to Youth: Solicitation, Harassment, and Problematic Content', Berkman Center for Internet & Society, Cambridge, p. 21, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/RAB_Lit_Review_121808_0.pdf.

3. UNICEF, 'Child Safety Online: Global Challenges and Strategies', Innocenti Research Centre, Florence, p. 30, www.unicef.org/pacificislands/ict_eng.pdf.

Foreword

The explosion of information and communication technology has created unprecedented opportunities for children and young people to communicate, connect, share, learn, access information and express their opinions on matters that affect their lives and their communities. But wider and more easily available access to the Internet and mobile technology also poses significant challenges to children's safety – both online and offline.

To reduce the risks of the digital revolution while enabling more children and young people to reap its benefits, governments, civil society, local communities, international organizations and the private sector must come together in common purpose.

The technology industry has a critical role to play in establishing the foundations for safer and more secure use of Internet-based services and other technologies – for today's children and future generations. Businesses must put protecting children at the heart of their work, paying special attention to protecting the privacy of young users' personal data, preserving their right to freedom of expression, and putting systems in place to address violations of children's rights when they occur. Where domestic laws have not yet caught up with international law, business has an opportunity – and the responsibility – to bring their business practices in line with those standards.

These new Guidelines for Industry on Child Online Protection provide a framework for the increasingly broad range of companies that develop, provide or make use of information and communication technologies in the delivery of their products and services. Such companies are especially well positioned to drive innovative solutions, creating digital platforms that can expand educational opportunities and enable children and young people both to engage in the civic life of their communities to become truly global citizens.

Local and national initiatives are critical, and we look forward to collaborating on complementary guidelines for governments that address the formulation, implementation, management and monitoring of Country Action Plans to strengthen child online protection.

The Internet knows no boundaries, and our efforts to protect children must be ambitious and far-ranging. We are grateful to our partners in the Child Online Protection (COP) Initiative and other organizations participating in the open consultation process for their invaluable support in developing these guidelines. We look forward to working with our partners in every sector to make child online protection a priority. And we hope these new Child Online Protection Guidelines will help create a safer and more secure world for all.

Dr Hamadoun I. Touré
Secretary-General
ITU

Mr. Anthony Lake
Executive Director
UNICEF

PART 1

Introduction, key areas and general guidelines

1.1. Purpose

The Child Online Protection (COP) Initiative is a multi-stakeholder network launched by the International Telecommunication Union (ITU) to promote awareness of child safety in the online world and to develop practical tools to assist governments, industry and educators.[4] As part of the initiative, in 2009, ITU published a set of COP Guidelines for four groups: children; parents, guardians and educators; industry; and policymakers. The Guidelines for Industry on Child Online Protection are aimed at establishing the foundation for safer and more secure use of Internet-based services and associated technologies for today's children and future generations. In response to substantial advances in technology and convergence, ITU, UNICEF and the COP partners have developed and updated the Guidelines for the broad range of companies that develop, provide or make use of telecommunications or related activities in the delivery of their products and services.

The new Guidelines for Industry on Child Online Protection are the result of consultations with members of the COP Initiative, as well as a wider open consultation that invited members of civil society, business, academia, governments, media, international organizations and young people to provide feedback on the Guidelines.

The Guidelines apply to the safety of children when using information and communication technologies (ICTs). They provide advice on how industry can work to help ensure children's safety when using the Internet or any of the associated technologies or devices that can connect to it, including mobile phones and game consoles. The purpose of this document is to:

- Establish a common reference point and guidance to the ICT and online industries and relevant stakeholders.
- Provide guidance to companies on identifying, preventing and mitigating any adverse impacts of their products and services on children's rights.

4. For more information, see, ITU 'Child Online Protection', www.itu.int/cop.

- Provide guidance to companies on identifying ways in which they can promote children's rights and responsible digital citizenship among children.
- Suggest common principles to form the basis of national or regional commitments across all related industries, while recognizing that different types of businesses will use diverse implementation models.

Part 1 offers general guidelines for industry on protecting children's safety when using information and communication technologies, along with recommendations for promoting positive ICT use, including responsible digital citizenship among children.

Part 2 offers sector-specific checklists that recommend actions to respect and support children's rights for the following sectors:

- Mobile operators
- Internet service providers
- Content providers, online retailers and applications (app) developers
- User-generated content, interactive and social media service providers
- National and public service broadcasters
- Hardware manufacturers, operating system developers and app stores.

1.2. Background

During the past 25 years, new information and communication technologies have profoundly changed the ways in which children interact with and participate in the world around them. The proliferation of Internet access points, mobile technology and the growing array of Internet-enabled devices – combined with the immense resources to be found in cyberspace – provide unprecedented opportunities to learn, share and communicate. The benefits of ICT usage include broader access to information about social services, educational resources and health information. As children and families use the Internet and mobile phones to seek information and assistance, and to report incidents of abuse, these technologies can help protect children from violence and exploitation. Information and communication technologies are also used to gather and transmit data by child protection service providers, facilitating, for example, birth registration, case management, family tracing, data collection and mapping of violence. Moreover, the Internet has increased access to information in all corners of the globe, offering children and young people the ability to research almost any subject of interest, access worldwide media, pursue vocational prospects and harness ideas for the future.

ICT usage empowers children to assert their rights and express their opinions, and it provides multiple ways to connect and communicate with their families and friends. In addition, information and communication technologies serve as a major mode of cultural exchange and a source of entertainment.

Despite the profound benefits of the Internet, children can also face a number of risks when using ICTs. Children can be exposed to inappropriate content for their age or to inappropriate contact, including from potential perpetrators of sexual abuse. They can suffer reputational damage associated with publishing sensitive personal information either online or through 'sexting', having failed to fully comprehend the implications for themselves and others of their long-term 'digital footprints'.

Children may be unaware of the short- and long-term consequences of engaging in risky or inappropriate behaviours that create negative repercussions for others and themselves. They also face risks related to online privacy in terms of data collection and usage and the collection of location information.

The Convention on the Rights of the Child, which is the most widely ratified international human rights treaty, sets out the civil, political, economic, social, and cultural rights of children.[5] It establishes that all children have a right to education; to leisure, play and culture; to obtain appropriate information; to freedom of thought and expression; to privacy and to express their views on matters that affect them in accordance with their evolving capacities. The Convention also protects children from all forms of violence, exploitation and abuse and discrimination of any kind and ensures that the child's best interest should be the primary consideration in any matters affecting them. Parents, caregivers, teachers and people in the community, including community leaders and a range of civil society actors, have the responsibility to nurture and support children in their passage to adulthood. Governments have the ultimate responsibility to ensure that parents, caregivers, teachers, community leaders and civil society actors may fulfil this role. Private sector actors, including the ICT industry, also have a key responsibility to fulfil children's rights.

Building on the United Nations Guiding Principles on Business and Human Rights,[6] the Children's Rights and Business Principles call on businesses to meet their responsibility to respect children's rights by avoiding any adverse impacts linked to their operations, products or services. The Principles also articulate the difference between respect – the minimum required of business to avoid causing harm to children – and support, for example, by taking voluntary actions that seek to advance the realization of children's rights.

When it comes to protecting children's rights online, businesses have to strike a careful balance between children's right to protection and their right to access to information and freedom of expression. Therefore companies must ensure that measures to protect children online are targeted and are not unduly restrictive, either for the child or other users. Moreover, there is growing consensus in relation to the importance of industry proactively promoting digital citizenship among children and devel-

5. United Nations, Convention on the Rights of the Child, New York, 20 November 1989, www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx. All but three countries – Somalia, South Sudan and the United States – have ratified the Convention on the Rights of the Child.

6. For more information and to access the full United Nations Guiding Principles document, see www.business-humanrights.org/UNGuidingPrinciplesPortal/Home.

oping products and platforms that facilitate children's positive use of ICTs.

Traditional distinctions between different parts of the telecommunications and mobile phone industries, and between Internet companies and broadcasters, are fast breaking down or becoming irrelevant. Convergence is drawing these previously disparate digital streams into a single current that is reaching billions of people in all parts of the world. Cooperation and partnership are the keys to establishing the foundations for safer and more secure use of the Internet and associated technologies. Government, the private sector, policymakers, educators, civil society, parents and caregivers each have a vital role in achieving this goal. Industry can act in five key areas, as described in section 1.3.

1.3. Five key areas for protecting and promoting children's rights

This section outlines five key areas where companies can take actions to protect children's safety when using ICTs and promote their positive use of ICTs.

Integrating child rights considerations into all appropriate corporate policies and management processes

Integrating child rights considerations requires that companies take adequate measures to identify, prevent, mitigate and, where appropriate, remediate potential and actual adverse impacts on children's rights. The United Nations Guiding Principles on Business and Human Rights call on all businesses to put in place appropriate policies and processes to meet their responsibility to respect human rights.

Businesses should pay special attention to children and youth as a vulnerable group in regards to data protection and freedom of expression. The United Nations General Assembly Resolution, "The right to privacy in the digital age" reaffirms the right to privacy and freedom of expression without being subjected to unlawful interference.[7,8] Additionally, the Human Rights Council Resolution on "The promotion, protection and enjoyment of human rights on the Internet", recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development and affirms the same rights people have offline must also be protected online.[9] In States which lack adequate legal frameworks for the protection of children's rights to privacy and freedom of expression, companies should follow enhanced due diligence to ensure policies and practices are in line with international law. As youth civic engagement continues to increase through online communications, companies have a responsibility to respect children's rights, even where domestic laws have not yet caught up with international standards.

Additionally, companies should have in place an operational-level grievance mechanism to provide a format for affected individuals to raise concerns of potential violations. Operational level mechanisms should be accessible to girls and boys, their families and those who represent their interests. Principle 31 of the Guiding Principles on Business and Human Rights clarifies that such mechanisms should be

7. United Nations General Assembly Resolution, "The right to privacy in the digital age", A/RES/68/167, www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

8. United Nations Human Rights Council "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue", www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

9. United Nations Human Rights Council Resolution, "The promotion, protection and enjoyment of human rights on the Internet", A/HRC/20/L.13, http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement

legitimate, accessible, predictable, equitable, transparent, rights-compatible, a source of continuous learning, and based on engagement and dialogue. Together with internal processes to address negative impacts, grievance mechanisms should ensure companies have frameworks in place to ensure children have suitable recourse when their rights have been threatened.

When companies take a compliance-based approach towards ICT safety that focuses on meeting national legislation, following international guidance when national legislation is not present, and the avoidance of adverse impacts on children's rights, companies proactively promote children's development and well-being through voluntary actions that advance children's rights to access information, freedom of expression, participation, education and culture.

Developing standard processes to handle child sexual abuse material

The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography defines 'child pornography' as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.[10] Of all child sexual abuse material analysed by the Internet Watch Foundation in 2013, 81 per cent of child victims appear to be 10 years of age or younger, and 51 per cent of the images depicted sexual activity between adults and children, including rape and torture.[11] These disturbing facts underscore the importance of collaborative action among industry, government, law enforcement and civil society to combat child sexual abuse material.

While many governments are tackling the dissemination and distribution of child sexual abuse material by enacting legislation, pursuing and prosecuting abusers, raising awareness, and supporting children to recover from abuse or exploitation, many countries do not yet have adequate systems in place. Mechanisms are required in each country to enable the general public to report abusive and exploitative content of this nature. Industry, law enforcement, governments and civil society must work closely with each other to ensure that adequate legal frameworks in accordance with international standards are in place. Such frameworks should criminalize all forms of child sexual abuse and exploitation, including through child abuse materials, and protect the children who are victims of such abuse or exploitation, and ensure that reporting, investigative and content removal processes work as efficiently as possible.[12]

Responsible companies are taking a number of steps to help prevent their networks and services from being misused to disseminate child sexual abuse material. These include placing language in terms and conditions or codes of conduct that explicitly forbid such content;[13] developing robust notice and takedown processes; and working with and supporting national hotlines.

Additionally, some companies deploy technical measures to prevent the misuse of their services or networks

10. United Nations, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, article 2, New York, 25 May 2000, www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx.

11. Internet Watch Foundation, 'Annual & Charity Report 2013', LINX, UK, https://www.iwf.org.uk/accountability/annual-reports/2013-annual-report

12. Industry should provide links to national hotlines from their websites. In places where a hotline is not yet established, industry could refer reporters to the International Association of Hotlines at www.inhope.org where any of the international hotlines can be selected to make a report.

13. It should be noted that inappropriate user conduct is not limited to child sexual abuse material and that any type of inappropriate behaviour or content should be handled accordingly by the company.

for sharing known child sexual abuse material. For example, some Internet service providers are also blocking access to URLs confirmed by an appropriate authority as containing child sexual abuse material if the website is hosted in a country where processes are not in place to ensure it will be rapidly deleted. Others are deploying hashing technologies to automatically locate images of child sexual abuse that are already known to law enforcement/hotlines.

Creating a safer and age-appropriate online environment

Very few things in life can be considered absolutely safe and risk free all of the time. Even in cities where the movement of traffic is highly regulated and closely controlled, accidents still happen. By the same token, cyberspace is not without risks, especially for children. Children can be thought of as receivers, participants and actors in their online environment. The risks that they face can be categorized into three areas:[14]

- *Inappropriate content* – Children may stumble upon questionable content while searching for something else by clicking a presumably innocuous link in an instant message, on a blog or when sharing files. Children may also seek out and share questionable material. What is considered harmful content varies from country to country, yet examples include content that promotes substance abuse, racial hatred, risk-taking behaviour or suicide, anorexia or violence.
- *Inappropriate conduct* – Children and adults may use the Internet to harass or even exploit other people. Children may sometimes broadcast hurtful comments or embarrassing images or may steal content or infringe on copyrights.
- *Inappropriate contact* – Both adults and young people can use the Internet to seek out children or other young people who are vulnerable. Frequently, their goal is to convince the target that they have developed a meaningful relationship, but the underlying purpose is manipulative. They may seek to persuade the child to perform sexual or other abusive acts online, using a webcam or other recording device, or they will try to arrange an in-person meeting and physical contact. This process is often referred to as 'grooming'.

Online safety is a community challenge and an opportunity for industry, government and civil society to work together to establish safety principles and practices. Industry can offer an array of technical approaches, tools and services for parents and children. These can include offering tools to develop new age-verification systems or to place restrictions on children's consumption of content and services, or to restrict the people with whom children might have contact or the times at which they may go online.

Some programmes allow parents to monitor the texts and other communications that their children send and receive. If programmes of this type are to be used,

14. Livingstone, S., and L. Haddon, 'EU Kids Online: Final report', EU Kids Online, London School of Economics and Political Science, London (EC Safer Internet Plus Programme Deliverable D6.5), June 2009, p. 10.

it is important this is discussed openly with the child, otherwise such conduct can be perceived as 'spying' and may undermine trust within the family.

Acceptable use policies are one way that companies can establish what type of behaviour by both adults and children is encouraged, what types of activities are not acceptable, and the consequences of any breaches to these policies. Reporting mechanisms should be made available to users who have concerns about content and behaviour. Furthermore, reporting needs to be followed up appropriately, with timely provision of information about the status of the report. Although companies can vary their implementation of follow-up mechanisms on a case-by-case basis, it is essential to set a clear time frame for responses, communicate the decision made regarding the report, and offer a method for following up if the user is not satisfied with the response.

Online content and service providers can also describe the nature of content or services they are providing and the intended target age range. These descriptions should be aligned with pre-existing national and international standards, relevant regulations, and advice on marketing and advertising to children made available by the appropriate classification bodies. This process becomes more difficult, however, with the growing range of interactive services that enable publication of user-generated content, for example, via message boards, chat rooms and social networking services. When companies specifically target children, and when services are overwhelmingly aimed at younger audiences, the expectations in terms of content and security will be much higher.

Companies are also encouraged to adopt the highest privacy standards when it comes to collecting, processing and storing data from or about children as children may lack the maturity to appreciate the wider social and personal consequences of revealing or agreeing to share their personal information online, or to the use of their personal information for commercial purposes. Services directed at or likely to attract a main audience of children must consider the risks posed to them by access to, or collection and use of, personal information (including location information), and ensure those risks are properly addressed. In particular, companies should ensure the language and style of any materials or communications used to promote services, provide access to services, or by which personal information is accessed, collected and used, aid understanding and assist users in managing their privacy in clear and simple ways.

Educating children, parents and teachers about children's safety and their responsible use of ICTs

Technical measures can be an important part of ensuring that children are protected from the potential risks they face online, but these are only one element of the equation. Parental control tools and awareness raising and education are also key components that will help empower and inform children of various age groups, as well as parents, caregivers and educators.

Although companies have an important role in ensuring that children use ICTs in the most responsible and safest possible way, this responsibility is shared with parents, schools, and children.

Many companies are investing in educational programmes designed to enable users to make informed decisions about content and services. Companies are assisting parents, caregivers and teachers in guiding children and adolescents towards safer, more responsible and appropriate online and mobile phone experiences. This includes signposting age-sensitive content and ensuring that information on items such as content prices, subscription terms and how to cancel subscriptions, is clearly communicated.

It is also important to provide information directly to children on safer ICT use and positive and responsible behaviour. Beyond raising awareness about safety, companies can facilitate positive experiences by developing content for children about being respectful, kind and open-minded when using ICTs and keeping an eye out for friends. They can provide information about actions to take if they have negative experiences such as online bullying or grooming, making it easier to report such incidents and providing a function to opt out of receiving anonymous messages.

Parents sometimes have less understanding and knowledge of the Internet and mobile devices than children. Moreover, the convergence of mobile devices and Internet services makes parental oversight more difficult. Industry can work in collaboration with government and educators to strengthen parents' abilities to support their children to behave as responsible digital citizens. The aim is not to transfer responsibility for children's ICT use to parents alone, but to recognize that parents are in a better position to decide what is appropriate for their children and should be aware of all risks in order to better protect their children and empower them to take action.

Information can be transmitted online and offline through multiple media channels, taking into consideration that some parents do not use Internet services. Collaborating with school districts to provide curricula on online safety and responsible ICT use for children and educational materials for parents is important. Examples include explaining the types of services and options available for monitoring activities, actions to take if a child is experiencing online bullying or grooming, how to avoid spam and manage privacy settings, and how to talk with boys and girls of different age groups about sensitive issues. Communication is a two-way process, and many companies provide options for customers to contact them to report issues or discuss concerns.

As content and services grow ever richer, all users will continue to benefit from advice and reminders about the nature of a particular service and how to enjoy it safely.

Promoting digital technology as a mode for increasing civic engagement

The Convention on the Rights of the Child, in article 13, states that "the child shall have the right to freedom of expression; this right shall in-

clude freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice." Companies can fulfil their respect for children's civil and political rights by ensuring that technology, legislation and policies developed to protect children from online harm do not have the unintended consequences of supressing their right to participation and expression or preventing them from accessing information that is important to their well-being.

At the same time, businesses can also support children's rights by offering mechanisms and tools to facilitate youth participation. They can emphasize the Internet's capacity to facilitate positive engagement in broader civic life, drive social progress, and influence the sustainability and resiliency of communities, for example, by participating in social and environmental campaigns and holding those in charge accountable. With the right tools and information, children and young people are better placed to access opportunities for health care, education and employment, and to voice their opinions and needs in schools, communities and countries. They can access information about their rights and make demands for information, whether in terms of the right to information on matters that affect them, such as their sexual health, or political and government accountability.

Companies can also invest in the creation of online experiences that are appropriate for children and families. They can support the development of technology and content that encourage and enable children and young people to learn, innovate and create solutions.

Companies can, in addition, proactively support children's rights by working to close the digital divide. Children's participation requires digital literacy – the ability to understand and participate in the digital world. Without this ability, citizens will not be able to participate in many of the social functions that have become 'digitized', including but not limited to filing taxes, supporting political candidates, signing online petitions, registering a birth, or simply accessing commercial, health, educational or cultural information. The gap between citizens who are able to access these forums and those who cannot due to a lack of Internet access or digital literacy will continue to widen – placing the latter groups at a significant disadvantage. Companies can support multimedia initiatives to provide the digital skills that children need to be confident, connected and actively involved citizens.

1.4. General guidelines for all related industry

Table 1 outlines broad guidelines for industry in identifying, preventing and mitigating any adverse impacts of products and services on children rights – and for promoting children's positive use of information and communication technologies. Note that not all the steps listed in table 1 will be appropriate across all companies; the sector-specific checklists in tables 2–7 will highlight those steps that are most relevant for individual business sectors.

TABLE 1. GENERAL GUIDELINES FOR ALL RELATED INDUSTRY

INTEGRATING CHILD RIGHTS CONSIDERATIONS INTO ALL APPROPRIATE CORPORATE POLICIES AND MANAGEMENT PROCESSES	**Industry can identify, prevent and mitigate the adverse impacts of ICTs on children's rights, and identify opportunities to support the advancement of children's rights by taking the following actions:**
	Ensure that a specific individual and/or a team is designated with responsibility for this process and has access to the necessary internal and external stakeholders. Provide this person/team with the authority to take the lead in raising the profile of child online protection across the company.
	Develop a child protection/safeguarding policy and/or integrate specific children's rights risks and opportunities into companywide policy commitments (e.g., human rights, privacy, marketing and relevant codes of conduct).
	Integrate due diligence on child online protection issues into existing human rights or risk assessment frameworks (e.g., at the corporate level, product or technology level, and/or at the country level) to determine whether the business may be causing or contributing to adverse impacts through its own activities, or whether adverse impacts may be directly linked to its operations, products or services or business relationships.
	Identify child rights impacts on different age groups as a result of company operations and the design, development and introduction of products and services – as well as opportunities to support children's rights.
	Draw upon internal and external expertise and consult with key stakeholders, including children, on child online safety mechanisms to obtain ongoing feedback and guidance on company approaches.
	In States which lack adequate legal frameworks for the protection of children's rights to privacy and freedom of expression, companies should ensure policies and practices are in line with international standards. (UN General Assembly Resolution, "The right to privacy in the digital age", A/RES/68/167)
	Ensure access to remedy by putting in place operational-level grievance and reporting mechanisms for any child rights violations (e.g., child sexual abuse material, inappropriate content or contact, breaches of privacy).
DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL	**In collaboration with government, law enforcement, civil society and hotline organizations, industry has a key role to play in combating child sexual abuse material by taking the following actions:**
	Put in place internal procedures to ensure compliance under local and international laws on combating child sexual abuse material. When national regulations do not provide sufficient protection, companies should seek to go above and beyond the national regulations and use their leverage to lobby for legislative changes to enable industry to take steps to combat child sexual abuse material.
	Use customer terms and conditions and/or acceptable use policies to explicitly state the company's position on the misuse of its services to store or share child sexual abuse material and the consequences of any abuse.
	Develop notice and take down (NTD) and reporting processes that allow users to report child sexual abuse material or inappropriate contact and the specific profile/location where it was discovered. Ensure a process is in place to act on those reports, and agree on procedures to capture evidence and remove abusive content. If a company is operating in markets with less developed regulatory and law enforcement oversight of these issues, it can refer reporters to the International Association of Hotlines at www.inhope.org/gns/home.aspx, where any of the international hotlines can be selected to make a report.

CREATING A SAFER AND AGE-APPROPRIATE ONLINE ENVIRONMENT	**Industry can help create a safer, more enjoyable digital environment for children of diverse ages by taking the following actions:**
	Employ appropriate technical measures – such as parental control tools, age-differentiated experiences with password-protected content, block/allow lists, purchase/time controls, opt-out functions, filtering and moderating[15] – to prevent underage access and exposure to inappropriate content or services. Where possible, consider the use of age verification to limit access to content or material that, either by law or policy, is intended only for persons above a certain age. At the same time, companies should recognize the potential for misuse of such technologies in ways that could restrict children's right to freedom of expression and access to information.
	In addition to the terms and conditions, communicate clear rules in accessible and easily understood language that emphasizes what behaviour is and is not acceptable on the service, and is particularly geared for young users and for their parents and caregivers. Be sure to state the consequences of breaking any of these rules.
	Ensure that content and services that are not age-appropriate for all users are: • classified in line with national expectations; • consistent with existing standards in equivalent media; • marked with prominent display options to control access; • offered together with age verification, where possible.
	Adapt and implement heightened default privacy settings for collection, processing, storage, sale and publishing of personal data, including location-related information and browsing habits, gathered from people under 18. Default privacy settings and information about the importance of privacy should be appropriate to the age of the users and the nature of the service.
	Offer clear reporting tools and develop a process to act on reports of inappropriate content, contact and misuse, and provide detailed feedback to service users on the reporting process.
	Align business practices with relevant regulations and advice on marketing and advertising to children. Monitor where, when and how children might encounter potentially harmful advertising messages intended for another market segment.

15. Within online spaces, there are three main degrees of moderation: pre-mod (nothing is published before approval of the moderator); post mod (comments are published, but the moderator can remove them as soon as anything unacceptable is noticed); reactive mod (check comments which moderators are alerted after publication by users - and sometimes by the hosts.

EDUCATING CHILDREN, PARENTS, AND TEACHERS ABOUT CHILDREN'S SAFETY AND THEIR RESPONSIBLE USE OF ICTS	**Industry can complement technical measures with educational and empowerment activities by taking the following actions:**
	Clearly describe available content and corresponding parental controls or family safety settings. Make language and terminology accessible, visible, clear and relevant for all users – including children, parents and caregivers – especially in relation to terms and conditions, costs involved in using content or services, privacy policies, safety information and reporting mechanisms.
	Educate customers on how to manage concerns relating to Internet usage – including spam, data theft and inappropriate contact such as bullying and grooming – and describe what actions customers can take and how they can raise concerns on inappropriate use.
	Set up mechanisms and educate parents to become involved in their children's ICT activities, particularly those of younger children, for example, providing parents with the ability to review children's privacy settings and with information on age verification.
	Collaborate with government and educators to build parents' abilities to support and speak with their children about being responsible digital citizens and ICT users.
	Based on the local context, provide materials for use in schools and homes to educate and enhance children's use of information and communication technologies and help children develop critical thinking that enables them to behave safely and responsibly when using ICT services.
PROMOTING DIGITAL TECHNOLOGY AS A MODE TO FURTHER CIVIC ENGAGEMENT	**Industry can encourage and empower children by supporting their right to participation through the following actions:**
	Establish written procedures that ensure consistent implementation of policies and processes that protect freedom of expression for all users, including children, as well as documentation of compliance with these policies.
	Avoid over-blocking of legitimate, developmentally appropriate content. In order to ensure that filtering requests and tools are not misused in ways that restrict children's access to information, be transparent about blocked content and establish a process for users to report inadvertent blocking; this process should be available to all consumers, including webmasters. Any reporting process should provide clear, responsible and adjudicated terms of service.
	Develop online platforms that promote children's right to express themselves; facilitate participation in public life; and encourage collaboration, entrepreneurship and civic participation.
	Develop educational content for children that encourages learning, creative thinking and problem solving.
	Promote digital literacy, capacity building and ICT skills to equip children, particularly children in rural and underserved areas, to utilize ICT resources and fully participate safely in the digital world.
	Collaborate with local civil society and government on national/local priorities for expanding universal and equitable access to information and communication technologies, platforms and devices – and the underlying infrastructure to support them.

PART 2

Sector-Specific Checklists

Part 2 offers recommendations for how businesses in specific sectors can respect and support children's rights online. It outlines how the common principles and approaches presented in table 1 can be implemented more specifically as they affect businesses in different sectors. The checklists are organized by the same key areas and, in some cases, will refer back to the general guidelines in table 1.

The following sector checklists are not exhaustive, but are intended as a starting point for companies to respect and support children's rights in the online sphere. Each of the sector checklists has been developed in collaboration with key contributors and, as a result, there are minor variations in the tables.

2.1. Mobile operators

Mobile operators enable access to the Internet as well as offer a range of mobile-specific data services. Many operators have already signed up to COP codes of practice, and offer a range of tools and information resources to support their commitments.

Table 2 provides guidance for mobile operators on policies and actions they can take to enhance child online protection and participation.

TABLE 2. COP CHECKLIST FOR MOBILE OPERATORS

INTEGRATING CHILD RIGHTS CONSIDERATIONS INTO ALL APPROPRIATE CORPORATE POLICIES AND MANAGEMENT PROCESSES	**Mobile operators can identify, prevent and mitigate the adverse impacts of ICTs on children's rights, and identify opportunities to support the advancement of children's rights.**
	Refer to the general guidelines in table 1.
DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL	**In collaboration with government, law enforcement, civil society and hotline organizations, mobile operators can play a key role in combating child sexual abuse material by taking the following actions:**
	Collaborate with government, law enforcement, civil society and hotline organizations to effectively handle child sexual abuse material and report cases to the appropriate authorities. If a relationship with law enforcement and a hotline is not already established, engage with them to develop processes together. Mobile companies may also provide ICT training for law enforcement. If a company is operating in markets with less developed legal and law enforcement oversight of this issue, it can refer reporters to the International Association of Internet Hotlines at www.inhope.org/gns/report-here.aspx where any of the international hotlines can be selected to make a report. Resources: The GSM Association (GSMA) has developed law enforcement training materials relating specifically to mobile. To get in contact the GSMA to access the documents listed, please email cop@itu.int.
	Work with internal functions such as customer care, fraud and security to ensure that the business can submit reports of suspected illegal content directly to law enforcement and hotlines. Ideally, this should be done in a way that does not expose front-line staff to the content and re-victimize the affected child/children. In situations where staff may be exposed to abusive material, implement a policy or programme to support staff resiliency, safety and well-being.

DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL (CONT'D)	Support law enforcement in the event of criminal investigations through such activities as capturing evidence. Make sure that terms of service and conditions state that the company will collaborate fully with law enforcement investigations in the event that illegal content is discovered or reported.
	Use terms of service and conditions to specifically prohibit using mobile services to store/share or distribute child sexual abuse materials. Make sure these terms clearly state that child sexual abuse material will not be tolerated.
	Promote reporting mechanisms for child sexual abuse material and make sure that customers know how to make a report if they discover such material. If a national hotline is available, offer a link to the hotline from the corporate website and from any relevant content services promoted by the company. Resource: Vodafone, 'Illegal Content', www.vodafone.com/content/parents/get-involved/illegal_content.html
	If a national hotline is not available, explore opportunities to set one up (see the GSMA INHOPE Hotlines guide in 'Resources' for a range of options, including working with INHOPE and the INHOPE Foundation or using the Internet Watch Foundation International back-office solution) – and/or develop internal processes for customer care staff to submit reports of questionable content to law enforcement and www.inhope.org. Resources: GSMA INHOPE, 'Hotlines: Responding to reports of illegal online content – A guide to establishing and managing a hotline organization'. This document includes information on the IWF Foundation (for countries that need support building up their own hotline), as well as IWF International's back office solution, OCSARP (for countries that want to offer reporting but do not yet need a full national hotline) http://www.gsma.com/publicpolicy/myouth/mobiles-contribution-to-child-protection/mobile-alliance
	Have processes in place to immediately remove or block access to child sexual abuse material – including notice and takedown processes to remove illegal content as soon as it is identified. Ensure that third parties with whom the company has a contractual relationship have similarly robust notice and takedown processes in place. Resources: GSMA Mobile Alliance Against Child Sexual Abuse Content, 'Obstructing the Use of the Mobile Environment by Individuals or Organisations Wishing to Consume or Profit from Child Sexual Abuse Content', www.gsma.com/publicpolicy/myouth/mobiles-contribution-to-child-protection/mobile-alliance 'Notice and Take Down Process Paper', www.gsma.com/publicpolicy/wp-content/uploads/2012/07/Mobilecontributiontonoticeandtakedown.pdf GSMA Mobile Alliance Against Child Sexual Abuse Content: Preventing mobile payment services from being misused to monetise child sexual abuse content', www.gsma.com/publicpolicy/myouth/mobiles-contribution-to-child-protection/mobile-alliance

CREATING A SAFER AND AGE-APPROPRIATE DIGITAL ENVIRONMENT	**Mobile operators can help create a safer, more enjoyable digital environment for children of diverse ages by taking the following actions:**
	Establish a clear set of rules that are prominently placed and echo key points from the terms of service and acceptable use guidelines. User-friendly language for these rules should define: • the nature of the service and what is expected of its users; • what is and is not acceptable in terms of harmful content, behaviours and language, as well as prohibiting illegal usage and the consequences appropriate to the level of any breach – for example, reporting to law enforcement or suspension of the user's account.
	Make it easy for customers to report concerns about misuse to customer care, with standard and accessible processes in place to deal with different concerns, for example, if a customer is receiving unwanted communications (spam, bullying) or has seen inappropriate content.
	Be transparent, giving customers clear information about the nature of the services that are offered, for example: • type of content/service and costs; • minimum age required for access; • availability of parental controls, including what the controls cover (e.g., network) or do not cover (e.g., Wi-Fi) and training for their use; • what type of user information is collected and how it is used. Resources: GSMA, 'Privacy Design Guidelines for Mobile Application Development', www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development ICT Coalition, www.ictcoalition.eu
	Provide technical controls that are appropriate for the services offered and are as easy as possible for end users to implement. Such controls might include: • the ability to block or filter access to the Internet through the company's networks, including 'own brand' or third-party services that are promoted by the company; • age verification if the company's own content or services include elements that are only legal or appropriate for adult users (e.g., certain games, lotteries).
	Promote national support services that enable children to report and seek support in the case of abuse or exploitation (see, for example, Child Helpline International: www.childhelplineinternational.org).

EDUCATING CHILDREN, PARENTS AND TEACHERS ABOUT CHILDREN'S SAFETY AND THEIR RESPONSIBLE USE OF ICTS	**Mobile operators can complement technical measures with educational and empowerment activities by taking the following actions:**
	Inform customers – including parents, caregivers, children – about the services offered, for example: • type of content offered and corresponding parental controls; • how to report abuse, misuse and inappropriate or illegal content; • how this report will be handled; • what services are age restricted; • safe and responsible behaviour when using 'own-brand' interactive services
	Engage with the broader issues around safe and responsible digital citizenship, e.g., online reputation and digital footprint, harmful content, grooming. Consider partnering with local experts such as children's non-governmental organizations, charities and parenting groups to help shape the company's messaging and reach the intended audience.
	If the business already works with children or schools – for example, through corporate social responsibility programmes – investigate whether this engagement could be extended to include educating children and teachers on child online protection messages.
PROMOTING DIGITAL TECHNOLOGY AS A MODE FOR TO FURTHER CIVIC ENGAGEMENT	**Mobile operators can encourage and empower children by supporting their right to participation.**
	Refer to the general guidelines in table 1. Resources: GSMA, 'mEducation', www.gsma.com/connectedliving/meducation; 'Mobile for Development', www.gsma.com/mobilefordevelopment including 'mWomen' http://www.gsma.com/mobilefordevelopment/programmes/mwomen
	Inform customers – including parents, caregivers, children – about the services offered, for example: • type of content offered and corresponding parental controls; • how to report abuse, misuse and inappropriate or illegal content; • how this report will be handled; • what services are age restricted; • safe and responsible behaviour when using 'own-brand' interactive services.
	Engage with the broader issues around safe and responsible digital citizenship, e.g., online reputation and digital footprint, harmful content, grooming. Consider partnering with local experts such as children's non-governmental organizations, charities and parenting groups to help shape the company's messaging and reach the intended audience.
	If the business already works with children or schools – for example, through corporate social responsibility programmes – investigate whether this engagement could be extended to include educating children and teachers on COP messages.

2.2. Internet service providers

Internet service providers act as both a conduit, providing access to and from the Internet, and a repository for data through their hosting, caching and storage services. As a result, they have been in the forefront of accepting responsibility for protecting children online.

Table 3 provides guidance for Internet service providers on policies and actions they can take to enhance child online protection and participation.

Internet access in public spaces

It is becoming increasingly common for municipalities, retailers, transportation companies, hotel chains and other businesses and organizations to provide Internet access via Wi-Fi hotspots. Such access is typically free or provided at minimal cost, and sometimes with minimal sign-on formalities, as a public service or by a company to attract customers to its premises or persuade more people to use its services.

Promoting Wi-Fi is a great way to spread Internet availability in a given area. Care needs to be taken, however, when such access is being provided in public spaces where children are likely to be present on a regular basis. Users need to be mindful that Wi-Fi signals might be available to passers-by and user data compromised. The Wi-Fi provider will therefore not always be able to support or supervise the use of an Internet connection it has supplied – and users need to take precautions not to share sensitive information over publicly available Wi-Fi.

In public spaces, Wi-Fi providers may want to consider additional measures to protect children. More specifically, they can:

- Proactively block access to web addresses known to contain content that is inappropriate for a wide audience, in addition to their efforts to block access to child sexual abuse material.
- Include clauses in terms and conditions of use that forbid the use of Wi-Fi service to access or display any material that may be unsuitable in an environment where children are present. The terms and conditions should also include clear mechanisms regarding the consequences of infringements of such rules.
- Take all measures to protect against unauthorized access such as manipulation/loss of personal data.
- Install filters on the Wi-Fi system to reinforce and underpin the policy on inappropriate material.
- Provide procedures and software to assist in the control and monitoring of children's access to Internet content.

TABLE 3. COP CHECKLIST FOR INTERNET SERVICE PROVIDERS

INTEGRATING CHILD RIGHTS CONSIDERATIONS INTO ALL APPROPRIATE CORPORATE POLICIES AND MANAGEMENT PROCESSES	**Internet service providers can identify, prevent and mitigate the adverse impacts of ICTs on children's rights, and identify opportunities to support the advancement of children's rights.**
	Refer to the general guidelines in table 1.
DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL	**In collaboration with government, law enforcement, civil society and hotline organizations, Internet service providers can play a key role in combating child sexual abuse material by taking the following actions:**
	Prohibit uploading, posting, transmitting, sharing or making available content that violates the rights of any party or infringes any local, state, national or international law.
	Communicate with national law enforcement agencies or the national hotline(s) to pass on reports of illegal child sexual abuse material as soon as the provider is aware of it. Make sure that internal procedures are in place to comply with reporting responsibilities under local and international laws. If a company is operating in markets with less developed regulatory and law enforcement oversight of this issue, it can refer reporters to the International Association of Internet Hotlines at www.inhope.org/gns/home.aspx, where any of the international hotlines can be selected to make a report.
	Have processes in place to immediately remove or block access to child sexual abuse material – including notice and takedown processes to remove illegal content as soon as it is identified. Ensure that third parties with whom the company has a contractual relationship have similarly robust notice and takedown processes in place. Link reports of abuse to the processes with a public service agreement on the response procedure and takedown times.
	Actively assess commercial content hosted on the company's servers, whether branded or contracted from third-party content providers, on a regular basis. Consider using such tools as hash scanning of known images, image recognition software or URL blocking to handle child sexual abuse material.
	Set up a reporting mechanism that offers clear information for its usage, for example, give guidance on the illegal content and conduct to be reported and clarify what materials cannot be attached with the report in order to avoid further distribution on the web.

CREATING A SAFER AND AGE-APPROPRIATE ONLINE ENVIRONMENT	**Internet service providers can help create a safer, more enjoyable digital environment for children of diverse ages by taking the following actions:**
	Identify customers' age where appropriate, implementing a suitable solution according to individual services. This will be particularly important when the service is subject to legal restrictions based on age.
	Consider presenting the reporting function on all web pages and services. Seek to standardize the company's approach to reporting abuse or other breaches of a website's or online service's terms and conditions. When they move from one site to another, it should not be necessary for children or their parents to learn a new set of processes to report issues.
	Consider providing mechanisms such as parental control software and tools that enable parents to manage their children's access to Internet resources, e.g., white lists, content filters, usage monitoring, contact management, time/program limits.
	Use terms of service/terms and conditions to specifically prohibit unacceptable behaviour and include a minimum user age.
	Where possible, promote national support services that parents and caregivers may use to report and seek support in the case of abuse or exploitation.
	Avoid harmful or inappropriate advertising content online, and establish disclosure obligations to customers for services with content that is intended for an adult audience and could be harmful to children.
	Ensure that data collection policies comply with relevant laws concerning children's privacy, including whether parental consent is required before commercial enterprises can collect personal information from or about a child.
EDUCATING CHILDREN, PARENTS AND TEACHERS ABOUT CHILDREN'S SAFETY AND THEIR RESPONSIBLE USE OF ICTS	**Internet service providers can complement technical measures with educational and empowerment activities by taking the following actions:**
	Within community guidelines for children, parents and caregivers, echo key messages from terms and conditions in user-friendly language. Within the service itself, at the point of uploading content, include 'reminders' about such topics as the type of content that is considered to be inappropriate.
	Provide parents with the necessary information to understand how their children are using ICT services, e.g., including how to handle issues related to harmful content and conduct, and be well-positioned to guide them towards responsible usage. This can be facilitated by use of tools and through interactions with school districts to provide online safety curricula for children and educational materials for parents.
	Provide children with information on safer Internet use. Consider setting up messages on the Internet service provider landing page, e.g., • "Never share any contact details, including your physical location and your phone number, with anyone you don't know in person." • "Never agree to get together with anyone you have met online on your own without consulting an adult first. Always tell a trusted friend about your whereabouts." • "Do not respond to bullying, obscene or offensive messages. But save the evidence – do not delete the message." • "Tell a trusted adult or a friend if you are uncomfortable or upset about something or someone." • "Never give away your account password or username! Be aware that other people online may give false information to convince you to share your private information."

PROMOTING DIGITAL TECHNOLOGY AS A MODE TO FURTHER CIVIC ENGAGEMENT	**Internet service providers can encourage and empower children by supporting their right to participation.**
	Refer to the general guidelines in table 1.

2.3. Content providers, online retailers and app developers

The Internet provides all types of content and activities, many of which are intended for children. Content providers, online retailers and app developers have tremendous opportunities to build safety and privacy into their offerings for children and young people.

Table 4 provides guidance for content providers, online retailers and applications developers on policies and actions they can take to enhance child online protection and participation.

TABLE 4. COP CHECKLIST FOR CONTENT PROVIDERS, ONLINE RETAILERS ANDAPP DEVELOPERS

INTEGRATING CHILD RIGHTS CONSIDERATIONS INTO ALL APPROPRIATE CORPORATE POLICIES AND MANAGEMENT PROCESSES	**Content providers, online retailers and apps developers can help identify, prevent, and mitigate adverse impacts of ICTs on children's rights, and identify opportunities to support the advancement of children's rights by taking the following actions:**
	Refer to the general guidelines in table 1
DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL	**In collaboration with government, law enforcement, civil society and hotline organizations, content providers, online retailers and apps developers can play a key role in combating child sexual abuse material by the following actions:**
	Be prepared to handle child sexual abuse material and report cases to the appropriate authorities. If a relationship with law enforcement and a national hotline is not already established, engage with them to develop processes together.
	Specify that the business will collaborate fully with law enforcement investigations in the event that illegal content is reported or discovered, and note details regarding such penalties as fines or cancellation of billing privileges.
	Have processes in place to immediately remove or block access to child sexual abuse material – including notice and takedown processes to remove illegal content as soon as it is identified. Ensure that where needed, operators ask for the opinion of experts (content providers, national bodies in charge of COP, etc.) before destroying illegal contents. Ensure that relevant third parties with whom the company has a contractual relationship have similarly robust notice and takedown processes in place.
	Work with internal functions such as customer care, fraud and security to ensure that business can submit reports of suspected illegal content directly to law enforcement and hotlines. Ideally, this should be done in a way that does not expose front-line staff to the content and re-victimize the affected child/children. To address situations where staff may be exposed to abusive material, implement a policy or programme to support staff resiliency, safety, and well-being.
	Include data retention and preservation policies in order to support law enforcement in the event of criminal investigations through such activities as capturing evidence. Document the company's practices for handling child sexual abuse material, beginning with monitoring and extending to the final transfer and destruction of the content. Include a list of all personnel responsible for handling the material in the documentation.
	Promote reporting mechanisms for child sexual abuse material and make sure that customers know how to make a report if they discover such content. If a national hotline is available, offer links to that hotline from the corporate website and from any relevant content services promoted by the company. If a company is operating in markets with less developed regulatory and law enforcement oversight of this issue, it can refer reporters to the International Association of Internet Hotlines at www.inhope.org/gns/home.aspx, where any of the international hotlines can be selected to make a report.

CREATING A SAFER AND AGE-APPROPRIATE ONLINE ENVIRONMENT	**Content providers, online retailers and app developers can help create a safer, more enjoyable digital environment for children of diverse ages by taking the following actions:**
	Work with others in the industry to develop content classification/age rating systems that are based on accepted national or international standards and consistent with approaches taken in equivalent media. Where possible, content classifications should be consistent across different media platforms, for example, a film trailer in a movie theatre and on a smartphone would show customers the same classifications.
	To help parents and others decide whether content is age-appropriate for children, build applications and services in all media to align with content rating systems. Adopt appropriate age-verification methods to prevent children from accessing age-sensitive content, sites, products or interactive services. Provide advice and reminders about the nature and age-classification of the content they are using.
	A company that offers audiovisual and multimedia services might want to provide a personal identification number (PIN) to users who seek to access content that can be harmful for children.
	Ensure transparency in terms of pricing for products and services, and information collected about users. Ensure that data collection policies comply with relevant laws concerning children's privacy, including whether parental consent is required before commercial enterprises can collect personal information from or about a child.
	Make sure that advertising or commercial communication is clearly recognizable as such.
	Supervise content made available online and adapt it to the user groups who are likely to access it, for example, by establishing appropriate policies for online advertising to children. If the content offering supports an interactive element, such as commenting, online forums, social networks, gaming platforms, chat rooms or message boards, communicate a clear set of 'house rules' in customer-friendly language within the terms of service and user guidelines.
EDUCATING CHILDREN, PARENTS AND TEACHERS ABOUT CHILDREN'S SAFETY AND THEIR RESPONSIBLE USE OF ICTS	**Content providers, online retailers and app developers can complement technical measures with educational and empowerment activities by taking the following actions:**
	Provide customers with specific and clear information about content, such as the type of content, age ratings/restrictions, strong language or violence – along with the corresponding parental controls that are available, how to report misuse and inappropriate or illegal content, and how reports will be handled. In the interactive world this information should be provided in form of content labels for each programme.
	Encourage adults, including parents and teachers, to be involved in children's online content consumption, so that they can assist and guide children in the choice of content when they are making a purchase, as well as help establish rules of behaviour.
	Provide rules of use in clear and accessible language that encourage children to be vigilant and responsible when they are navigating the Internet.
	Build age-appropriate tools such as tutorials and help centres. Work with online/in-person prevention programmes and counselling clinics when appropriate. For example, if there is a risk of children becoming obsessively engaged with technology such as games, making it difficult for them to develop personal relationships or take part in healthy physical activities, a site could provide a contact link for a helpline or counselling service.

PROMOTING DIGITAL TECHNOLOGY AS A MODE TO FURTHER CIVIC ENGAGEMENT	**Content providers, online retailers and app developers can encourage and empower children by supporting their right to participation through the following actions:**
	Develop and/or offer a range of high-quality content that is age-appropriate. In addition to being attractive and usable, reliable and safe, such content can contribute to children's physical, mental and social development by providing new opportunities to entertain and educate.
	Provide information about a service to highlight the benefits the child would obtain by behaving well and responsibly, such as using the service for creative purposes.

2.4. User-generated content, interactive and social media service providers

There was a time when the online world was dominated by adults, but it is now clear that children and adolescents are major participants, on multiple platforms, in creating and sharing in the explosion of user-generated content.

Table 5 which has been adapted from the rules applied by one of the largest social network provides guidance for user-generated content, interactive and social media service providers on policies and actions they can take to enhance child online protection and participation.

TABLE 5. COP CHECKLIST FOR USER-GENERATED CONTENT, INTERACTIVE AND SOCIAL MEDIA SERVICE PROVIDERS

INTEGRATING CHILD RIGHTS CONSIDERATIONS INTO ALL APPROPRIATE CORPORATE POLICIES AND MANAGEMENT PROCESSES	**User-generated content, interactive and social media service providers can identify, prevent and mitigate the adverse impacts of ICTs on children's rights, and identify opportunities to support the advancement of children's rights.**
	Refer to the general guidelines in table 1.
DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL	**In collaboration with government, law enforcement, civil society and hotline organizations, user-generated content, interactive and social media service providers can play a key role in combating child sexual abuse material by taking the following actions:**
	All sites should have procedures in place to provide immediate assistance to law enforcement during emergencies and for routine inquiries.
	Specify that the business will collaborate fully with law enforcement investigations in the event that illegal content is reported or discovered, and note details regarding such penalties as fines or cancellation of billing privileges.
	Work with internal functions such as customer care, fraud and security to ensure that the business can submit reports of suspected illegal content directly to law enforcement and hotlines. Ideally, this should be done in a way that does not expose front-line staff to the content and re-victimize the affected child/children. To address situations where staff may be exposed to abusive material, implement a policy or programme to support staff resiliency, safety and well-being.
	Use terms of service and conditions to prohibit illegal content and behaviour, highlighting that: • illegal content, including child sexual abuse material, will not be tolerated; • the company will collaborate fully with law enforcement investigations in the event that illegal content is reported or discovered.
	Document the company's practices for handling child sexual abuse material, beginning with monitoring and extending to the final transfer and destruction of the content. Include a list of all personnel responsible for handling the material in the documentation.
	Adopt policies regarding ownership of user-generated content, including the option to remove user-created content at the user's request. Remove content that violates the provider's policies and alert the user who has posted it about the violation.
	Indicate that a user's failure to comply with policies for acceptable use will have consequences, including: • removal of content, suspension or closure of their account; • revoking a user's ability to share particular types of content or use certain features; • referring issues to law enforcement.

DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL (CONT'D)	Promote reporting mechanisms for child sexual abuse material or any other illegal content and make sure that customers know how to make a report if they discover such content. Build systems and provide trained staff to assess issues on a case-by-case basis and take appropriate action. Establish comprehensive and well-resourced user-support operation teams. Ideally, these teams would be trained to handle different types of incidents in order to ensure that adequate response is provided and appropriate actions are taken. When the user files a complaint, depending on the type of incident, it will be routed to appropriate staff. The company might also set up special teams to handle user appeals for instances when reports may have been filed in error.
	Have processes in place to immediately remove or block access to child sexual abuse material – including notice and takedown processes to remove illegal content as soon as it is identified. Ensure that third parties with whom the company has a contractual relationship have similarly robust notice and takedown processes in place. If legislation allows the material can be kept for evidence of a crime in case of investigations.
	Develop technical systems that can detect known illegal content and can prevent it from being uploaded, including to private groups, or flag it for immediate review by the company's safety team. Where possible, create proactive technical measures to analyse the objects and metadata linked to a profile to detect criminal behaviour or patterns, and take action appropriately.
	If the application or service allows customers to upload and store photographs on servers that are owned or operated by the company, have processes and tools in place to identify images that are most likely to contain child sexual abuse material. Consider proactive identification techniques such as scanning technology or human review.
CREATING A SAFER AND AGE-APPROPRIATE ONLINE ENVIRONMENT	**User-generated content, interactive and social media service providers can help create a safer, more enjoyable digital environment for children of diverse ages by taking the following actions:**
	Communicate in customer-friendly language within the terms of service and user guidelines a clear set of 'house rules' that define: • the nature of the service and what is expected of its users; • what is and is not acceptable in terms of harmful content, behaviours, language as well as prohibiting illegal usage; • consequences of any breach, for example, reporting to law enforcement and suspension of the user's account.
	Key safety and legal messages should be presented in an age-appropriate format (i.e. utilizing intuitive icons and symbols) both at signup and in a timely manner as different actions are taken on the site.
	Make it easy for customers to report concerns about misuse to customer care, with standard and accessible processes in place to deal with different concerns – for example, if a customer is receiving unwanted communications (spam, bullying) or has seen inappropriate content.
	Provide age-appropriate content sharing and visibility settings. For example, make privacy and visibility settings for children more restrictive than the settings for adults by default.
	Enforce minimum age requirements, and support the research and development of new age-verification systems such as biometrics, using known international standards for the development of such tools. Take steps to identify and remove underage users who have misrepresented their age to gain access. If they are not already in place, set up appropriate sign-on processes to determine whether users are old enough to access the content or service, and use nationally established age-verification systems linked to a reporting function or a help desk/centre that can help encouraging users to report people who have falsified their ages.

CREATING A SAFER AND AGE-APPROPRIATE ONLINE ENVIRONMENT (CONT'D)	Protect younger users from uninvited communication, and ensure that privacy and information-collection guidelines are in place.
	Find ways to review hosted images and videos, and delete inappropriate ones when found. Tools such as hash scanning of known images and image recognition software are available to assist with this. Photos and videos can be pre-checked to make sure that children do not publish sensitive personal information about themselves or others.
	A number of measures may be used to control access to user-generated content and protect children online against inappropriate or illegal content. Make sure that secure passwords are used as a step towards protecting children in gaming and other social media settings. Other techniques include: • giving parents the ability to control who contacts their children; • reviewing discussion groups to find harmful subject matter, hate speech and illegal behaviour, and deleting such content when it is found to violate the terms of use; • developing tools that actively to seek and remove content that is illegal/in breach of the company's terms of condition and service, as well as tools to prevent uploading of known illegal content to the site; • pre-moderating message boards with a team of specialized children's moderators who screen for content that is in contradiction to the published 'house rules' – each message can be checked before it is published, and moderators will also spot and flag suspicious users, as well as users in distress; • a team of community hosts who serve as the first point of contact for the moderators when they have concerns about a user.
	Be responsible for reviewing commercial content, including in forums, social networks and gaming sites. Implement appropriate standards and rules to protect children from age-inappropriate advertising, and establish clear limits for online advertising to children.
EDUCATING CHILDREN, PARENTS AND TEACHERS ABOUT CHILDREN'S SAFETY AND THEIR RESPONSIBLE USE OF ICTS	**User-generated content, interactive and social media service providers can complement technical measures with educational and empowerment activities by taking the following actions:**
	Create a section dedicated to safety tips, articles, features and dialogue about digital citizenship, as well as links to useful content from third-party experts. Safety advice should be easily spotted and provided in easy-to-understand language. Platform providers are also encouraged to have a uniform navigation interface across different devices, such as computers, tablets or mobile phones.
	Offer parents clear information about the types of content and services available – including, for example, an explanation of social networking sites and location-based services; how the Internet is accessed via mobile devices; and the options available for parents to apply controls.
	Inform parents about how to report abuse, misuse, and inappropriate or illegal content, and how the report will be handled. Let them know what services are age restricted, along with other ways to behave safely and responsibly when using interactive services.
	Establish a 'trust and reputation'-based system to encourage good behaviour and enable peers to teach best practices to each other by example. Promote the importance of social reporting, which allows people to reach out to other users or trusted friends to help resolve a conflict or open a conversation about troubling content.
	Provide advice and reminders about the nature of a given service or content and how to enjoy it safely. Build community guidelines into interactive services, for example, with safety pop-ups that remind users of appropriate and safe behaviour such as not giving out their contact details.

PROMOTE DIGITAL TECHNOLOGY AS A MODE TO FURTHER CIVIC ENGAGEMENT	**User-generated content, interactive and social media service providers can encourage and empower children by supporting their right to participation.**
	Refer to the general guidelines in table 1.

2.5. National and public service broadcasting

Children and young people are a significant audience for content developed by broadcasting services, which is increasingly accessible online. National and public service broadcasters are working to offer the same level of security for online viewing that is applied to television and radio.

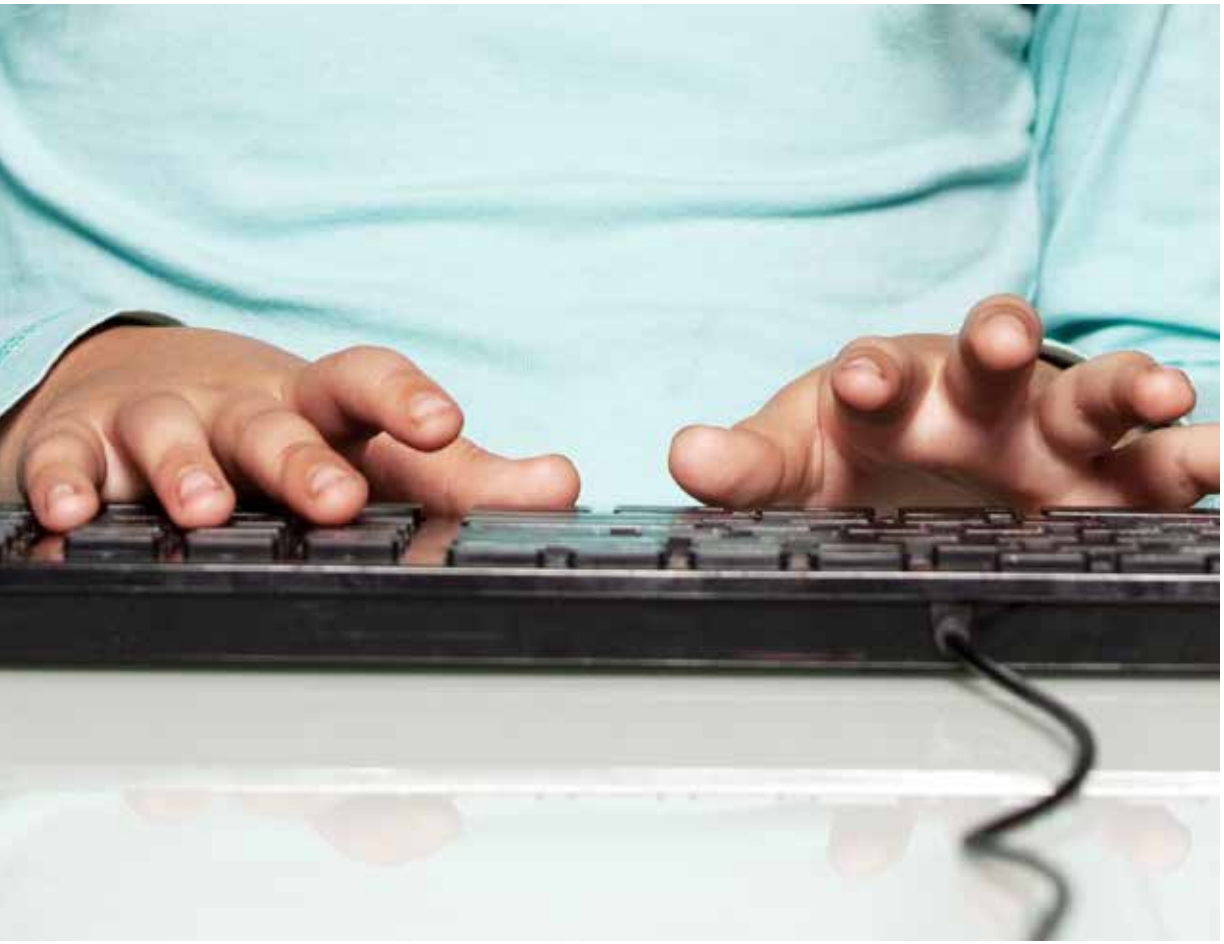
Table 6 provides guidance for national and public service broadcasters on policies and actions they can take to enhance child online protection and participation.

TABLE 6. COP CHECKLIST FOR NATIONAL AND PUBLIC SERVICE BROADCASTING

INTEGRATING CHILD RIGHTS CONSIDERATIONS INTO ALL APPROPRIATE CORPORATE POLICIES AND MANAGEMENT PROCESSES	**National and public service broadcasters can identify, prevent and mitigate the adverse impacts of ICTs on children's rights, and identify opportunities to support the advancement of children's rights by taking the following actions:**
	Develop policies that safeguard the welfare of children who contribute content online, in accordance with licensing agreements to consider the physical/emotional welfare and dignity of people under 18 who are involved in programmes (irrespective of consent that might have been given by a parent or other adult).
	Nominate a child protection policy manager or other designated person who can be contacted in relation to child online protection issues. If a child is at risk of harm, the child protection policy manager should immediately alert the appropriate authorities.
DEVELOPING STANDARD PROCESSES FOR HANDLING CHILD SEXUAL ABUSE MATERIAL	**In collaboration with government, law enforcement, civil society and hotline organizations, national and public service broadcasters have a key role to play in combating child sexual abuse material by taking the following actions:**
	In cases of child sexual abuse material, staff should contact the executive management team that is responsible for reporting it to the appropriate authorities. In addition: • alert national law enforcement agencies immediately; • alert their manager and report the material to the child protection policy manager; • contact the internal investigation service by phone or email with details of the incident and to ask for advice; • wait for advice from the relevant agency before deleting the material, saving it to a shared space or forwarding it. If the material is uploaded on a non-broadcaster space, it should be reported directly to an organization specialized in Internet safety that operates a hotline reporting system for members of the public and information technology professionals to report specific forms of potentially illegal online content.
	Implement a swift and robust escalation strategy if, for example, child sexual abuse material is posted or illegal conduct is suspected. Towards this end: • offer users a simple, easily accessible method of alerting the broadcaster to breaches of any rules of the online community; • remove content that breaks the rules; • take special care to mitigate risk around content, contact and conduct when running interactive online spaces designed to appeal to children; • before uploading broadcaster material onto a social networking site, be aware of the site's terms and conditions. Be sensitive to minimum age requirements on different social networking sites. The terms and conditions of each online space should also include clear mechanisms of reaction to infringements of such rules. Before uploading broadcaster material onto a social networking site, be aware of the site's terms and conditions.

CREATING A SAFER AND AGE-APPROPRIATE ONLINE ENVIRONMENT	**National and public service broadcasters can help create a safer, more enjoyable digital environment for children of diverse ages by taking the following actions:**
	Ensure that website moderators and hosts are prepared to remove content that breaks the site's 'house rules'. Hosts can improve the user experience for children by encouraging positive behaviour and defusing disputes before they get out of hand.
	Ensure pre-moderation of interactive spaces designed for children; active hosting can encourage an atmosphere where bullying and harassment are not acceptable. Unacceptable behaviour includes: • posting nasty or threatening comments on someone's profile; • setting up fake profiles or hate sites to humiliate a victim; • sending chain messages and attachments with harmful intent; • hacking into someone's account to send offensive messages to others.
	Take special precaution with staff members or collaborators who work with children – including anyone moderating a public electronic interactive communication service that is likely to be used wholly or mainly by children. These roles could require a preliminary criminal records check with police authorities.
	Decide what level of engagement is desired before launching a website, online profile or web page. Sites aimed to appeal children should only present content that is suitable for a young audience; if in doubt, the national authorities in charge of child protection may be consulted.
	Provide clear and factual content labelling. Be mindful that users can arrive at inappropriate content by following links on third-party sites that bypass the broadcaster home page or other contextualizing pages.
	Refer any incident of suspected grooming promptly to the online or interactive executive management team that is responsible for reporting it to the appropriate authorities: • make sure that a team member is available by phone when online interactive services are aimed to a young audience – the number should also be accessible via the broadcaster's switchboard; • establish common email addresses linked to the function (not the names) of team members to automatically alert those on duty of incidents; • when a content producer refers a report of suspected grooming to the interactive executive management team, she or he should also report it to the nominated child protection policy manager; • make it possible for users of the broadcaster's site to report suspected grooming incidents directly to authorities.
	Prioritize the safety and well-being of the child at all times. Always act within professional boundaries and ensure all contact with children is essential to the programme, event, activity or project. Never take sole responsibility for a child; if a child needs care, alert the parent or chaperone. Listen to and respect children at all times. If anyone is behaving inappropriately around children, report the concern to the local child protection contact at the broadcaster.

EDUCATING CHILDREN, PARENTS AND TEACHERS ABOUT CHILDREN'S SAFETY AND THEIR RESPONSIBLE USE OF ICTS	**National and public service broadcasters can complement technical measures with educational and empowerment activities by taking the following actions:**
	Make safety information, including advice links, prominent, easily accessible and clear when online content is likely to appeal to a high proportion of children.
	Offer a parental guidance tool, such as a 'lock' for control of content that can be accessed through a particular browser.
	Cooperate with parents to ensure that information disclosed on the Internet about children does not put them at risk. How children are identified in broadcasters' content requires careful consideration and will vary according to the context. Obtain children's informed consent when featuring them, wherever possible, and respect any refusal to take part.
PROMOTING DIGITAL TECHNOLOGY AS A MODE TO FURTHER CIVIC ENGAGEMENT	**National and public service broadcasters can encourage and empower children by supporting their right to participation.**
	Provide children with challenging, educational, enjoyable and interesting content that helps them make sense of the world in which they live. *Refer to the general guidelines in table 1.*



2.6. Hardware manufacturers, operating system developers and app stores

Children today are accessing the Internet through an array of electronic devices, from laptops to tablets to cell phones and beyond. Hardware manufacturers can provide built-in technical mechanisms along with educational and empowerment activities in order to promote a safer online environment for children.

Table 7 provides guidance for hardware manufacturers, operating system developers and app stores on policies and actions they can take to enhance child online protection and participation.

TABLE 7. COP CHECKLIST FOR HARDWARE MANUFACTURERS, OPERATING SYSTEM DEVELOPERS AND APP STORES

INTEGRATING CHILD RIGHTS CONSIDERATIONS INTO ALL APPROPRIATE CORPORATE POLICIES AND MANAGEMENT PROCESSES	**Hardware manufacturers, operating system developers and app stores can identify, prevent and mitigate the adverse impacts of ICTs on children's rights, and identify opportunities to support the advancement of children's rights.**
	Refer to the general guidelines in table 1.
DEVELOPING STANDARD PROCESSES TO HANDLE CHILD SEXUAL ABUSE MATERIAL	**In collaboration with government, law enforcement, civil society and hotline organizations, hardware manufacturers, operating system developers and app stores can play a key role in combating child sexual abuse content by taking the following actions:**
	Refer to the general guidelines in table 1
CREATING A SAFER AND AGE-APPROPRIATE ONLINE ENVIRONMENT	**Hardware manufacturers, operating system developers and app stores can help create a safer, more enjoyable digital environment for children of diverse ages by taking the following actions:**
	Use terms and conditions to draw users' attention to content in the company's online services, such as app stores, that might not be appropriate for all ages, whether originating from the manufacturer or from a third party. The terms and conditions should also include clear mechanisms for reporting and dealing with infringements of such rules.
	Offer easy-to-use parental control options that allow parents to restrict the services and content children can access when using electronic devices. These restrictions can include Internet access, access to social media, application/game purchase and installation, and use of location services.

EDUCATING CHILDREN, PARENTS AND TEACHERS ABOUT CHILDREN'S SAFETY AND THEIR RESPONSIBLE USE OF ICTS	**Hardware manufacturers, operating system developers and app stores can complement technical measures with educational and empowerment activities by taking the following actions:** Support customers by making guidelines available for family online safety, encouraging parents and caregivers to: • become familiar with products and services children are using; • ensure moderate use of electronic devices by children as part of a healthy and balanced lifestyle; • pay close attention to children's behaviour in order to identify changes that could indicate cyberbullying or harassment.
PROMOTING DIGITAL TECHNOLOGY AS A MODE TO FURTHER CIVIC ENGAGEMENT	**Hardware manufacturers, operating system developers and app stores can encourage and empower children by supporting their right to participation.** *Refer to the general guidelines in table 1.*

International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int/cop

Printed in Switzerland
Geneva, 2014

ISBN 978-92-61-15111-9

With the support of:

TELECOM ITALIA
Microsoft
UNODC United Nations Office on Drugs and Crime
unicri advancing security, serving justice, building peace
CHIS
SONY
cofface CONFEDERATION OF FAMILY ORGANISATIONS IN THE EUROPEAN UNION
OPTENET Get optimal internet
TREND MICRO
GSMA Mobile Alliance Against Child Sexual Abuse Content
IWF Internet Watch Foundation
ecpat
INTERPOL
vodafone
EBU