GUIDELINES FOR INDUSTRY ON CHILD ONLINE PROTECTION

Respecting and Supporting Children's Rights

Input Requested on the Draft Guidelines

Initiative Overview

The ITU Child Online Protection (COP) (http://www.itu.int/osg/csd/cybersecurity/gca/cop/) is a multi-stakeholder initiative to promote awareness of the importance of child safety in the online world and to develop practical tools to assist governments, industry and educators in this domain. As part of the initiative, a set of Child Online Protection Guidelines has been prepared by ITU in collaboration with the COP partners for the following stakeholder groups: Children, Parents, Guardians and Educators, Industry, Policy Makers. The current "Guidelines for Industry on Child Online Protection (COP)" were introduced four years ago and the need for an updated and broader set of guidelines has been evident for some time due to substantial advances in technology, convergence and regulation. The review process to update the current COP Guidelines for Industry was initiated in early 2013 by the COP members together with UNICEF and ITU taking the lead in editing, co-ordination and consultation. The draft Guidelines are intended to be now more aligned with the UN Guiding Principles on Business and Human Rights (UNGPs) and also to reflect the specific issues related to the ICT sub-sectors.

The draft guidelines have been developed through an initial consultation of the ITU COP members and it was agreed that a broader consultation is needed to gain more feedback especially on the sub-sector elements of the guidelines, and to gain support for the document. The online consultation aims to engage diverse audiences across all regions - seeking substantive inputs to the draft Guidelines themselves, the themes on which the Guidelines are based and building support and fostering commitment for the Guidelines. The public online consultation process is hosted via the Business and Human Rights Resource Centre website http://www.business-humanrights.org and in addition to the online consultation, the draft Guidelines will be presented and are open for a public consultation at the IGF 2013 (Internet Governance Forum) in Bali, Indonesia in October and at the ITU Telecom World 2013 in Bangkok, Thailand in November 2013. All the consultations are held in English.

Instructions for feedback

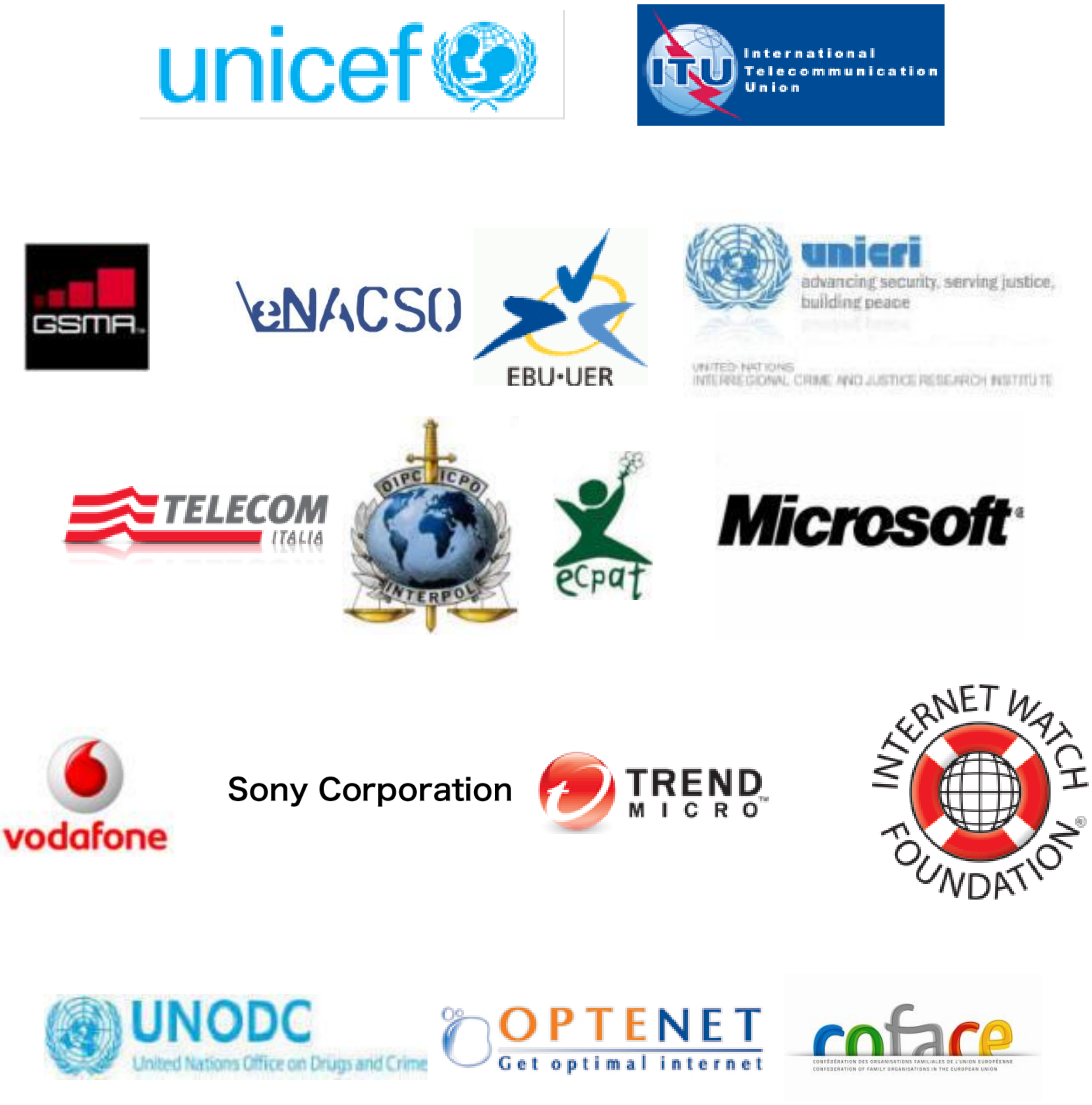
Please find following the *Draft Guidelines for Industry on Child Online Protection* and a set of questions at the end to facilitate your input and feedback on the draft. The partner organizations are looking forward to receiving your responses by 20 December 2013. Responses can be sent to the following mailbox: cop@itu.int and csr@unicef.org . This feedback will provide input into the development of the final Guidelines for Industry on Child Online Protection, which will be released in January 2014.

In the event you wish further background and context prior to responding, please contact the UNICEF CSR unit in Geneva on csr@unicef.org or ITU COP on cop@itu.int.

We appreciate your valuable time and support for the initiative!

GUIDELINES FOR INDUSTRY ON CHILD ONLINE PROTECTION

The following organizations have contributed to the drafting of these Guidelines:


unicef
ITU International Telecommunication Union
GSMA
eNACSO
EBU·UER
unicri advancing security, serving justice, building peace
UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE
TELECOM ITALIA
OIPC ICPO INTERPOL
ecpat
Microsoft
vodafone
Sony Corporation
TREND MICRO
INTERNET WATCH FOUNDATION
UNODC United Nations Office on Drugs and Crime
OPTENET Get optimal internet
coface
CONFÉDÉRATION DES ORGANISATIONS FAMILIALES DE L'UNION EUROPÉENNE
CONFEDERATION OF FAMILY ORGANISATIONS IN THE EUROPEAN UNION

Glossary of terminology

Internet and associated technologies: Depending on the context in this document, the term "Internet and associated technologies" refers to a broad range of companies that not only provide Internet services but develop products or services that make use of Internet platforms. Given the increasing trend towards vertical integration, many hardware manufacturers are now content providers. Internet Service Providers (ISPs) aside from continuing to offer access to cyberspace will also often provide facilities to allow for the publication of user generated content. More and more companies are offering their customers a number of options to take advantage of an array of devices, software and services. Therefore, depending on the context, the following terms are often used interchangeably: "Internet and associated technologies", "ICT and online industries", "Internet-based services" to encompass the rich and complex tapestry that is the modern internet. These guidelines will also have some relevance to sectors which straddle or are outside of a number of the traditional ICT industries, in particular media and other companies which provide online content.

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 their products; provide their services; apply leverage through business relationships with key stakeholders and partners; and exert their influence on economic and social development. Under the *UN Guiding Principles on Business and Human Rights*, companies have a responsibility to take adequate measures to identify, prevent, mitigate, and where appropriate, remediate their potential or actual negative impacts on human rights. The *Children's Rights and Business Principles*[1] call on companies to respect children's rights and avoid any infringement on the rights of children, and address any adverse child rights impact with which the business is involved. In addition, the Principles 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.

Child sexual abuse material: The term 'child sexual abuse material' is used to refer to recorded images of children subjected to sexual abuse and exploitation. These images might be in the form of stills, videos or be available via streaming.

While the term "child pornography" is used commonly in legislation and international conventions, this term is not used in the guidelines because "pornography" is commonly 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 abuse materials, and its use can therefore cause misunderstanding.

Child: The Convention on the Rights of the Child, defines a child as every human being below the age of 18 years unless, under the country-specific law applicable to the child, majority is attained earlier.[2]

Adolescent: UNICEF and partners define adolescents as people between the ages of 10 and 19.

Youth/Young People: The United Nations define youth as persons between the ages of 15 and 24.

[1] Recognizing a need for explicit guidance about what it means for business to respect and support children's rights, the UN Global Compact, Save the Children and UNICEF—together with companies and other stakeholders—released a set of ten Principles on Children's Rights and Business ('the Principles') in March 2012. Building upon the UN Guiding Principles, the Principles identify a comprehensive range of actions that all business should take to prevent and address risks to children's rights and maximize positive business impact in the workplace, marketplace and the community.

[2] Convention on the Rights of the Child, 1989,http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx

Purpose and Background

Purpose

The Guidelines for Industry on Child Online Protection have been prepared in the context of the Child Online Protection (COP) Initiative in order to establish the foundations for safer and more secure Internet-based services and associated technologies not only for today's children but also for future generations. These 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 many associated technologies or devices which can connect to it or use it, including mobile phones and games 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
- Provide guidance to companies on identifying ways in which they might promote children's rights and responsible digital citizenship among children and young people.
- Suggest common principles that, though requiring different models of implementation for different industry players, could potentially form the basis of national or regional pan-industry commitments.

This document is divided into two parts: Part 1 outlines broad guidelines for industry on the protection of children's safety when using ICTs, and also provides advice on the role that technology can play in positively promoting responsible digital citizenship among children and young people. Part 2 offers sector specific checklists for ICT industry that recommend actions to respect and support children's rights for the following sectors:

- Mobile operators
- Internet access in public spaces
- ISPs
- Public Broadcasting Service providers
- Content providers, online retailers and apps developers
- User generated content, interactive, social media service providers
- Hardware manufacturers

Background

Over the past twenty years, new information and communication technologies (ICTs) have profoundly changed the ways in which today's young people 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 children and young people with unprecedented opportunities to learn, share and communicate.

The benefits of ICTs, among other things, include broader access to social services, educational resources and health information. ICTs also help to protect children from violence, exploitation and abuse since children and families use the Internet and mobile phones to seek information and assistance, and to report violence. Increasingly ICTs 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 young people the ability to research virtually any subject of interest, access worldwide media, pursue vocational prospects, and harness ideas for the future.

ICTs have empowered children to assert their rights, express their views and opinions, and have also improved their ability to connect and communicate with their families and friends. Last but not least, ICTs increasingly serve as a major mode of cultural exchange and as a source of entertainment.

Yet despite the profound benefits of the Internet, children and young people nonetheless can face a number of risks through 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 their long-term ‘digital footprints’. In that respect ICTs can therefore harm children who themselves may engage in risky or inappropriate behaviours such as bullying that create negative repercussions for others and themselves, without being fully aware of the short or long term consequences.

The Convention on the Rights of the Child (CRC), which is the most widely ratified international human rights treaty,[3] protects children from all forms of violence, exploitation and abuse, including sexual exploitation and abuse. It also establishes that all children have a right to education, leisure, play and culture; the right to obtain appropriate information and to express their views in matters that affect them as well as to freedom of thought and expression, privacy and non-discrimination.. While Governments have the primary responsibility to ensure that children’s rights are met, other stakeholders such as parents and other caretakers, teachers, community leaders, civil society actors and the private sector including the ICT industry, all have a responsibility in fulfilling children’s rights.

Businesses’ duties to fulfil these rights are set out in *Children’s Rights and Business Principles*, which calls on business to meet their *responsibility to respect* children’s rights both by avoiding any adverse impacts linked to their operations, products or services, and also by encouraging companies to go beyond a “do-no-harm” approach through adopting a *commitment to support* the advancement of children’s rights.

Finding an appropriate balance between ensuring that all children have access to ICTs and at the same time as ensuring that they are protected from violence, abuse and exploitation while using ICTs, can be challenging. There is growing consensus that industry should not only tackle problems in relation to children’s use of ICTs but should proactively promote digital citizenship among children, and help to 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 hitherto disparate digital streams into a single current that is reaching out to billions of people in all parts of the world. Co-operation and partnership are the keys to establishing the foundations for safer and more secure use of the Internet and associated technologies not only for today’s children but also for future generations. Government, the private sector, policymakers, educators, civil society and parents each have a role to play. Industry can act in five key areas: 1) Integrate child rights considerations into all appropriate corporate policies and management processes; 2) Develop processes for handling child sexual abuse content; 3) Develop safer and age appropriate online environments; 4) Educate children, parents, and teachers about children’s safety and responsible use of ICTs ; 5) Promote digital technology as a mode to further positive civic engagement.

[3] All but three States (Somalia, South Sudan and the United States) have ratified the CRC,

Part I: Five Key Areas for Protecting and Promoting Children's Rights

Part 1 outlines broad guidelines for the protection of children's safety when using ICTs and the promotion of their positive use of ICTs according to five key areas, introduced below.

1) **Integrate child rights considerations into all appropriate corporate policies and management processes**

Integrating children's rights considerations requires that companies take adequate measures to identify, prevent, mitigate, and where appropriate, remediate potential and actual risks to infringing on children's rights. The *Children's Rights and Business Principles* call for all businesses to put in place appropriate policies and processes, as set out in the *UN Guiding Principles on Business and Human Right*s, which facilitate the prevention and mitigation of adverse impacts of ICTs on children's rights. They also call on companies to identify opportunities to proactively support children's rights. The *Principles* articulate the difference between companies' responsibility to respect children's rights—the minimum required of business to avoid causing harm to children; and support them—for example by taking voluntary actions that seek to advance the realization of children's rights. Rather than taking a compliance-based, or do-no-harm approach towards children's rights and ICT safety, companies that are providing Internet-based services and associated technologies to children have the opportunity to advance children's development and well-being in ways that facilitate their rights, not least their rights to access information, freedom of expression, participation, education and culture.

Companies can operationalize their respect and support for children's rights in several ways starting with relevant policy commitments, e.g. to human rights, privacy and child online protection. They can also carry out due diligence with respect to child rights impacts by including such considerations into human rights, social or product-level assessments, then integrating and acting upon the findings, tracking responses and communicating how impacts are addressed. Finally, where businesses have identified that they have caused or contributed to adverse impact, then they should provide for or cooperate in their remediation through internal processes or by working with appropriate external agencies, or both.

2) **Develop processes for handling child sexual abuse content**

The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography defines child abuse material 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. Of all child sexual abuse content analysed by the Internet Watch Foundation in 2012, 81 per cent of child victims appear to be 10 years of age or under and 53 per cent of the images depicted sexual activity between adults and children including rape and sexual torture.[4] These disturbing facts underscore the importance of collaborative action amongst industry, government and law enforcement to combat child sexual abuse content.

While many individual governments are tackling the dissemination and distribution of child sexual abuse content through enacting legislation, pursuing and prosecuting abusers, raising awareness, and supporting

[4] http://www.iwf.org.uk/resources/trends

children to recover from abuse or exploitation, many countries have inadequate systems in place. Mechanisms are required in each country to enable the reporting of child abuse content by members of the public. Industry, law enforcement and governments should work closely with each other to ensure that the necessary legal framework is in place and that reporting, investigative and content removal processes work as efficiently as possible.

Responsible companies are taking a number of additional steps to help prevent their networks and services from being misused to disseminate child sexual abuse content. These may include placing additional language in Terms and Conditions or Codes of Conduct that explicitly forbid child sexual abuse content, developing robust Notice and Take Down processes[5], deploying hashing technologies to automatically locate images of child sexual abuse content that is already known to law enforcement/hotlines and working with and supporting national hotlines. Additionally, Internet companies should provide mechanisms for customers to report abuse and invest in innovation for improved detection. A growing number of ISPs are also now blocking access to URLs confirmed by an appropriate authority as containing child sexual abuse content if the material is hosted in another country where processes are not in place to ensure it will be deleted rapidly.

NOTE: It should be noted that user conduct is not limited to child sexual abuse and that any type of inappropriate behaviour and/or content should be handled accordingly by the companies.

3) Develop 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 young children. Children can be thought of as a receiver, participant and actor in their online environment.

The risks that children face can be categorized into three areas that include:

- Inappropriate content. Children may stumble upon questionable content while searching for something else by clicking a presumably innocuous link in an instant message, blog or when sharing files. Young people may also seek out and share questionable material.

- Inappropriate conduct. Children and adults too, may use the Internet to harass or exploit other people. Children and young people may sometimes broadcast hurtful comments or embarrassing images or may steal or infringe on copyright.

- 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 them that they have a meaningful relationship but the underlying purpose is to manipulate them into performing sexual or other abusive acts either in real life following a meeting, or online using a web cam or some other recording device. This process is often referred to as *grooming*.

Online safety is a community challenge, and industry, governments and others should work together to establish safety principles. Industry can offer an array of technical approaches, tools and services for parents and children. These might include offering tools for parents and caregivers to place restrictions on their child's consumption of content and services, or to restrict the people with whom their children might have contact or the times at which they may go online.

[5] Notice and Take Down' (NTD) - Operators and service providers are sometimes notified of suspect content online by customers, members of the public or by law enforcement or hotline organisations. If the report comes from a member of the public, the information is passed on to law enforcement or national hotline, as appropriate, for confirmation of whether the content is illegal or to take any further legal action. When issued with a NTD notice, operators and service provider takes steps to have the illegal content removed.

Online content and service providers can develop methods to describe the nature of content or services they are providing and the intended target age-range. Wherever possible these should be aligned with the pre-existing relevant national standards or advice made available by the appropriate classification bodies. However, with the growing range of interactive services which allow for user generated content to be published (e.g. via message boards, chat rooms, and social networking services) this becomes a lot more difficult. When companies specifically target children and young people and when services are overwhelmingly aimed at younger audiences, then the expectations in terms of content and security will be that much higher.

Conformance with relevant regulations and advice on marketing and advertising to children. Companies can commit to providing transparent, clear and age appropriate information about the costs of products or services which children might buy and be clear about what data is being collected and how it will be used. Moreover, online advertisers are encouraged to adopt the highest privacy standards when it comes to collecting, processing and storing data of, from or about children.

By employing acceptable use policies, companies can establish what type of behaviour is encouraged by both adults and children, what types of activities are forbidden, and the consequences of any violations.

Reporting mechanisms should be made available to users in order to report concerns. Studies show that the majority of young people are aware that they can report, but do not have sufficient skills, knowledge or confidence in the process actually to do it. Furthermore, reporting needs to be followed up appropriately, with information about the status of the report being provided in a timely way. There should be a clear time frame for responses, information about the decision made about the reporting and a possibility to follow up should the response not satisfy the user. NOTE: Companies can vary the implementation of the above follow-up mechanisms on a case-by-case basis.

4) Educate children, parents, and teachers about children's safety and responsible use of ICTs

Technical measures such as filtering software can play an important part in ensuring that children are protected from the potential risks they face online, but these are only one part of the equation. Awareness raising and education efforts are a key component. These will help empower and inform children, parents, other caregivers and educators. While companies have an important role to play in ensuring that children and young people use ICTs in the most responsible and safest possible way, it is a shared responsibility. Industry, parents, schools and children and young people themselves all have a key part to play.

Companies do invest in education programs designed to enable users to make informed decisions about the content and services they use. Efforts also include assisting parents, caregivers and teachers to guide young children and adolescents towards safer, more responsible and appropriate online and mobile phone experiences. This includes signposting age-sensitive content, but also ensuring clarity of communication with regard, for example, to pricing of content, subscription terms and how to cancel subscriptions.

It is also important to provide information directly to children on safer use of ICTs and encouraging positive and responsible behaviours in their digital lives. Beyond raising awareness about safety, companies can help 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 themselves. Moreover, the convergence of mobile phones and Internet services makes parental oversight much 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 responsible use of ICTs to parents alone, but to recognize that parents 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 - some parents do not use Internet services—so collaborating with school districts to provide curricula for online safety and responsible use of ICTs for children and educational materials for parents is important. Examples include explaining the types of services and the options available to apply monitoring activities, actions to take if a child is experiencing online bullying or grooming, how to avoid spam, and manage privacy settings.

As content and services grow ever richer, all users will continue to benefit from advice and reminders about the nature of a given service they are using and how to enjoy it safely. Communication is, of course, a two-way process and many companies now provide options for customers to contact them to report issues or discuss concerns.

5) Promote digital technology as a mode to further positive civic engagement

Companies can also go beyond a “do-no-harm” approach to proactively support the rights of children to express their opinions and access appropriate information through their use of the Internet and associated technologies. Companies can emphasize the Internet’s capacity to facilitate the positive engagement of children and young people in broader civic life and in contributing towards finding solutions to the many challenges facing us all in the modern world. Article 13 of the *s Convention on the Rights of the Child* articulates that “The child shall have the right to freedom of expression; this right shall include 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.”

Digital and mobile technology, when used safely, can give children and adolescents the chance to make a difference. As digital citizens, children can exercise their right to express their opinions, bring forward their problems and needs, and interact in the life of their communities, for example, by participating in important social and environmental campaigns and holding those in charge accountable. They can access information about their rights and make demands for information, whether in terms of political and government accountability or the right to information on matters that affect them, such as their sexual health. Companies can proactively support children’s rights to participation by offering mechanisms and tools for youth participation and working to close the digital divide. They can support the development of technology and content that encourages and enables young people to innovate, create solutions, drive social progress and directly influence the sustainability and resilience of their communities. With the right tools and information, young people are better placed to access opportunities for healthcare, education and employment, to voice their opinions in schools, communities and countries.

Children’s participation requires digital literacy and the ability to understand and participate in the digital world. The inability to interact in the digital world may result in the inability of citizens to participate in many social functions that have become digitized (e.g. filing taxes, supporting political candidates, signing online petitions, registering a birth, or simply accessing commercial, health, educational or cultural information, and the list goes on). The gap between citizens who are able to access these fora and those that cannot due to a lack of Internet access or digital literacy will widen placing the latter groups at a significant disadvantage. Companies can support multi-media initiatives to provide the digital skills that children need to be confident, connected and actively involved citizens.

General Guidelines for all Related Industry

The following table outlines broad guidelines for the ICT industry for identifying, preventing and mitigating any adverse impacts of their products and services on children rights and the promotion of children's positive use of ICTs.

Integrate child rights considerations into all appropriate corporate policies and management processes	**Industry should identify, prevent and mitigate the adverse impacts of ICTs on children's rights, and identify opportunities to support the advancement of children's rights**
	Ensure that responsibility for this area lies with a specific individual and/or ream who has access to the necessary internal and external stakeholders and has been given sufficient authority to take a lead in raising the profile of child online protection across the organization Hire more staff to moderate content and provide adequate training.
	Identify child rights impacts on different age groups as a result of company operations, and the design, development and introduction of new products and services, as well as opportunities to support children's and young people's rights through the company's service provision.
	Draw upon internal and external expertise and consult with key stakeholders, including young people, on child online safety mechanisms to ensure that services that are seen as effective and easy to use by young people.
	For full transparency consider publishing annual reports with data disclosures on child protection issues.
Develop processes for handling child sexual abuse content	**In collaboration with governments, law enforcement and hotline organisations, industry has a key role to play in combating child sexual abuse content by engaging in the following actions:**
	Put in place internal procedures to ensure compliance under local and / or international laws with regard to child sexual abuse content.
	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 content and the consequences of any abuse.
	Develop reporting processes that allow users to report child sexual abuse content and the specific profile / location where it was discovered.
	Proactively communicate with local or national law enforcement agencies and national hotlines to report child abuse materials and agree procedures to capture evidence and

	remove content.
Develop a safer and age appropriate service environment	**Industry can help to offer a safer, more enjoyable digital environment through the following actions:**
	Employ appropriate technical measures such as age-verification, block/allow lists, spend/time controls, opt out functions, filtering and moderating to prevent under age access and exposure to age-inappropriate content or services; work to keep services provided exclusively for children adult-free.
	In addition to the Terms and Conditions, communicate clear house rules by emphasizing in accessible and easily understood language what behavior is and is not acceptable on the service, particularly for young users and for their parents and caregivers, and the consequences of any breach.
	Ensure that content and services that are not age-appropriate for all users are classified in line with national expectations, are consistent with existing standards in equivalent media, and are offered together with age-verification, where possible.
	Where appropriate, set up the default privacy settings of services in such a way as to protect children online (e.g. higher privacy settings by default for the collection, processing and storage of data of people under 18).
	Offer reporting tools and processes for inappropriate content or contact and/or misuse and provide detailed feedback on the reporting process to the users.
	Conform with relevant regulations and advice on marketing and advertising to children.
Educate children, parents, and teachers about children's safety and responsible use of ICTs	**Industry can complement technical measures with educational and empowerment activities through the following actions:**
	Clearly describe the content that is available and the corresponding parental controls or family safety settings. Make language and terminology accessible and visible, clear and relevant for all users, including children, young people, parents and caregivers, especially in relation to the Terms and Conditions, costs involved in using the content or services, privacy policy, safety information and reporting mechanisms.
	Educate customers on how to manage concerns relating to Internet usage generally – including areas such as Spam, data theft, and inappropriate contact e.g. 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 (e.g. ability to review their children's privacy settings, working age-verification, etc.).
	Work in collaboration with government and educators to build parents' abilities to support their children to behave as responsible digital citizens and ICT users.

	Based on an understanding of the local context, provide materials for use in schools and homes to educate and enhance children’s use of ICTs and develop their critical thinking that enable them to behave safely and responsibly when using ICTs.
Promote digital technology as a mode to further positive civic engagement	**Industry can encourage and empower children’s right to participation by:**
	Establish written procedures that ensure consistent implementation of policies and processes that protect freedom of expression for all users, including children, and documenting compliance with these policies.
	Develop content and applications that promote children’s rights to express themselves, facilitate participation in public life, and encourage learning, creative thinking, problem solving, collaboration, entrepreneurship and civic participation.
	Promote digital literacy, capacity building and ICT skills to equip children, particularly children in rural areas and underserved areas, to utilize ICT resources and fully participate in the digital world.
	Collaborate with local civil society and government on national/local development priorities on expanding universal and equitable access to ICT technologies, platforms and devices and the underlying infrastructure to support them.

Part 2, below, outlines how the common principles and approaches in the table above might be implemented more specifically as they affect organisations in different sectors.

Part 2: Sector-Specific Checklists

This section offers sector-specific checklists that recommend actions to respect and support children's rights in the online world.

Mobile Operators

As discussed in Part 1 of this document, the ultimate goal is for COP considerations to be become part of "Business As Usual" activities. To begin with, this will take time and commitment: stakeholders across the business will need to be educated as to how COP may impact their area of responsibility.

The 'checklist' below will help those mobile operators who are just beginning to develop their COP programme to focus on key areas as they get started. There is further reading (case studies, additional guidance, etc.) associated with many of the items listed below – this can be accessed by following the relevant links.

Mobile Operator Child Online Protection Checklist		Case studies
Integrate child rights considerations into all appropriate corporate policies and management processes	**Industry should 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 General Guidelines	
Develop standard processes for handling child sexual abuse content	**In collaboration with government and law enforcement, mobile operators can play a key role in combating child sexual abuse content by the following actions:**	
	It is vital to collaborate with Law Enforcement (LE) and appropriate hotlines in order to effectively handle issues related to child sexual abuse content. • If your organisation does not yet have working relationships with LE and (if applicable) the national hotline in this area, you will need to engage with them and develop processes together. • If appropriate, it may be useful for your organisation to provide training for LE on the use of mobiles / ICTs etc.	The GSMA has developed LE training materials relating specifically to mobile: Mobile operators can contact Samantha Lynch sam.lynch@gsma.com for access to the materials.
	You will also need to work with the appropriate functions within your organisation (e.g. customer care, fraud / security) to ensure that you are able to:	

	• Pass on reports of suspected illegal content directly to LE / hotlines– ideally this should be done in such a way that your front line staff are not exposed to the content • Support LE in the event of criminal investigations (e.g. capture evidence)	
	Use Terms of Service / Terms and Conditions to specifically prohibit child sexual abuse content or behaviours: • Check whether your organisation's ToS / T&C adequately reflect the following: o Illegal content, including child sexual abuse content, will not be tolerated o Your organisation will collaborate fully with LE investigations in the event that illegal content is reported / discovered	
	Promote reporting mechanisms for child sexual abuse content: • In the event that your customers discover child sexual abuse content, do you have a reporting mechanism you can promote to them? E.g. o If your country has a hotline, can you offer links to that hotline from your corporate website and / or from any relevant content services promoted by your organisation? o If your country does not have a hotline, are there opportunities to set one up or develop internal processes for customer care staff to pass on reports of suspect content to LE?	How to report illegal content' by Vodafone GSMA / INHOPE guide to setting up a hotline
	Have processes in place to swiftly remove or block access to child sexual abuse content: • Develop Notice and Take Down processes to remove illegal content as soon as it has been identified, and confirmed as illegal and appropriate to remove.	GSMA Mobile Alliance- Notice and Take Down Paper
	Contact Samantha Lynch sam.lynch@gsma.com, if you would like a copy of 'Toolkit: Responsible approach to combating the use of mobile services to access child sexual abuse content'.	
Develop a safer and age appropriate service environment	**Mobile operators can help to offer a safer, more enjoyable digital environment through the following actions:**	
	Developing a clear set of "House Rules", reflected in Terms of Service and Acceptable Use Guidelines (which echo key points from the ToS in user friendly language, placed prominently within the service) for services they offer, which define:	

	• The nature of the service and what is expected of its users • What is and is not acceptable in terms of content / behaviours / language etc. This would prohibit any illegal usage – but this is also an opportunity to ban swearing, bullying, etc. • Consequences of any breach (suspension of account, report to LE etc.)	
	It is important to be transparent, giving your customers clear information about the nature of the services you are offering, for example: • What type of content / service is on offer? • What is the minimum age required to access this service? • What user information is collected and how is it used? • What costs are involved? • If you offer parental controls, what is covered (e.g. network) and what is not (e.g. Wi-Fi)?	Privacy Design Guidelines for Mobile Application Development
	Customers should be able to report concerns about misuse to customer care, and there should be processes in place to deal with different concerns – for example, if a customer is receiving unwanted communications (spam, bullying) or has seen inappropriate content. What technical controls might be appropriate for the services you have on offer and how easy it is for these to be adopted or implemented by end users? For example: • The ability to block or filter access to the internet through your networks (whether 'own brand' or third party services that you could promote from your site) • Age-verification if you are offering content or services (e.g. certain games, lottery, etc.) which may only be legal or appropriate for adult users	
Educate children, parents, and teachers about children's safety and responsible use of ICTs	**Mobile operators can complement technical measures with education and empowerment activities through the following actions:**	
	Tell customers (parents, carers, children) what they need to know about your services specifically, for example: • What type of content is on offer, what corresponding parental controls are available • How to report abuse / misuse / inappropriate or illegal content… • … and how this report will be handled • What services are age-restricted • How to behave safely and responsibly when using 'own-brand' interactive services	

	In order to engage with the broader issues around safe and responsible digital citizenship (e.g. managing reputation and 'digital footprint', harmful content, grooming), it might be helpful to partner with local experts (e.g. children's NGOs / charities, parenting groups) to help shape your messaging and help you reach your audience. If your organisation already works with children or schools (e.g. through CSR programmes) you could investigate whether the scope of these engagement could be extended to include educating children / teachers on COP messages.	
Promote digital technology as a mode tofurther positive civic engagement	**Industry can encourage and empower children's right to participation by:**	
	Refer to General Guidelines	**GSMA mEducation** **GSMA Mobile for development** **Apps for Good**

Internet access in public spaces

It is becoming increasingly common for municipalities, retailing businesses, transportation companies, hotel chains and other organizations to provide internet access via Wi-Fi hotspots. Typically such access will be free or it will be provided at minimal cost and perhaps with minimal sign on formalities. The internet access is provided either as a public service or as a way of attracting more customers to a company's premises or of persuading more people to use their services.

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

In public spaces Wi-Fi providers will not want to provide children or young people with the means to access age-inappropriate material. Neither will they want to risk their internet connection being used by anyone else to expose children and young people to age inappropriate content. In some countries major retailers and transportation companies have understood the importance of this issue and have decided to do two things:

Public Access Child Online Protection Checklist		**Case studies**
Integrate child rights considerations into all appropriate corporate policies and management processes	**Industry should 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 General Guidelines	
Develop processes for handling child sexual abuse content	**In collaboration with government and law enforcement, companies and organisations offering Internet access in public spaces can play a key role in combating child sexual abuse content by the following actions:**	
	Block access to web addresses known to contain illegal content	
Develop a safer and age appropriate service	**Companies and organisations offering Internet access in public spaces can help to offer a safer, more enjoyable digital environment through the following actions:**	
	Include in Terms and Conditions of Use clauses which forbid the use of WiFi service to access or display any material which may be unsuitable for display in an environment where children and young people are	

environment	present.	
	Install filters on the WiFi system to reinforce and underpin the policy.	
Educate children, parents, and teachers about children’s safety and responsible use of ICTs	**Companies and organisations offering Internet access in public spaces can complement technical measures with education and empowerment activities through the following actions:**	
	Refer to General Guidelines	
Promote digital technology as a mode to further positive civic engagement	**Industry can encourage and empower children’s right to participation by:**	
	Refer to General Guidelines	

Internet access: Internet Service Providers

Internet Service Providers have long accepted that they have a distinct responsibility with regards to child online protection. This is largely due to the fact that ISPs act as both a conduit, providing access to and from the Internet, and a repository because of the hosting, caching and storage services which they provide.

The ‘checklist’ below will help those internet service providers who want to develop their COP programme to focus on key areas as a good starting point of their policies. There is further reading (case studies, additional guidance, etc.) associated with many of the items listed below – this can be accessed by following the relevant links.

Internet Service Providers Child Online Protection Checklist		**Case studies**
Integrate child rights considerations into all appropriate corporate policies and management processes	**Industry should 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 General Guidelines	
Develop standard processes for handling child sexual abuse content	**In collaboration with government, law enforcement, and hotline organisations, internet service providers can play a key role in combating child sexual abuse content by the following actions:**	
	Prohibit uploading, posting, transmitting, sharing or making available content that would constitute or instruct for a criminal offence, violate the rights of any party or any local, state, national or international law.	
	Proactively communicate with national law enforcement agencies or the national hotline to pass on reports of illegal child sexual abuse content as soon as the provider is aware of it. • Do you have internal procedures in place to ensure that they comply with their responsibilities under local and / or international laws?	
	Develop Notice and Take Down processes to remove illegal content as soon as it has been identified, and confirmed as illegal and appropriate to remove. • You should link reports of abuse to “Notice and Take Down”	

	processes – with a public service level agreement on the response or take down times • Do you actively assess commercial content hosted on your own servers (either branded content or content from contracted third party content providers) on a regular basis? • Is it appropriate to use tools such as hash scanning and image recognition software or URL blocking on your service?	
Develop a safer and age appropriate service environment	**Internet Service Providers can help to offer a safer, more enjoyable digital environment through the following actions:**	
	Wherever possible and appropriate identify the age of customers. • Implement a suitable solution appropriate to the individual service (this will be particularly important where the service in question is subject to legal restrictions based on age). • Establish disclosure obligations to customers for services whose content are intended for an adult audience that could be harmful to minors. Consider making the ability to report a default presence on all web pages and services by means of a "report abuse button" to the extent possible. • A common, recognisable button could be developed which will be always in the same location on every screen. • A proper web form, which is accessible via specific links in the footer of the institutional sites. • Appropriate abuse desk mailboxes. The reporting mechanism should offer indications and clear information for its usage: for example, it could give clear guidance on the material to be reported; moreover, it should clarify when some materials cannot be attached to avoid any distribution on the web. Avoid harmful or inappropriate advertising content online.	
	Consider having mechanisms, such as parental control software, which enable parents to manage their children's access to Internet resources. Some examples could be: White Lists, Content filters, Usage monitoring, Contact management, Time/program limits, "safe search" (Practice varies and attitudes towards it vary. In the UK every mobile phone provider has restricted access to adult content by default since 2005. It can be removed by completing an age verification process. Several ISPs are likely to do the same and WiFi providers are doing it as we speak!).	
	Use Terms of Service / Terms and Conditions to specifically prohibit unacceptable behaviours. Where possible, promote national support services where parents and carers may report and seek support in the case of abuse and	

	exploitation.	
Empower and educate children, parents, other caregivers, and teachers about children's safety and responsible use of ICTs	**Internet Service Providers can complement technical measures with education and communication activities through the following actions:**	
	Echo key messages from their Terms and Conditions in user-friendly language in community guidelines (including children, young people, parents and caregivers) and 'reminders' that sit within the service itself – for example, by reminding users of the types of content which are considered inappropriate at the point of uploading content. Provide parents with the necessary information to understand how their children are using ICT services (e.g. including issues such a bullying) and be well-positioned to guide them towards responsible usage. This can be facilitated by the use of tools and interactions with school districts to provide online safety curricula for children and educational materials for parents.	
	Children can be also provided with information related on safer Internet use. Internet Service Providers could for example provide information in their landing page such as: • "Never give away your physical or any other contact details e.g. your mobile phone number" • "Never agree to meet anyone you have met online in person, especially without consulting an adult first" • "Do not respond to inappropriate (bullying, obscene, or offensive) messages and save the evidence, don't delete it" • "Tell an adult if you are uncomfortable or upset about something or someone" • "Never give away your account password or username; and be aware that other players may give false information about real-world characteristics." Where possible, you should also promote national support services where children may report and seek support in the case of abuse and exploitation.	
Promote digital technology as a mode to further positive civic engagement	**Industry can encourage and empower children's right to participation by:**	
	Refer to General Guidelines	FOSI's Platform for Good

Public Broadcasting Service Providers

Public broadcasting (and broadcasting sector in general) has been traditionally one of the most controlled and regulated sector of the industry. Normally this is not a sector from which there are threats to the Child protection.

But since when the broadcasting signals and its contents are distributed or made accessible also on-line, new problems arise and potential areas of risk emerged. The Broadcasting sector (and especially PSBs) are re-elaborating all previous defences in order to continue to ensure the level of security that they provided through TV and radio signals, also in the on line world.

The “check-list” below will help those broadcasters that are expanding more and more their services in the on line (or “non-linear”) world to avoid some of the most frequent traps they could fall in.

Background:

Children[6] and young people are very important to the Public Service broadcasting, because they are one of the main targets indicated in the Public Service Remit. Children contribute and interact with PSB in many different ways - as contributors, actors, presenters, through our interactive and user generated content, via all platforms. In the mission of most of PSB around the world there is to provide this audience with challenging, educative, enjoyable and interesting content and to help them make sense of the world in which they live.

Public Broadcasting Service Providers Child Online Protection Checklist		**Case studies**
Integrate child rights considerations into all appropriate corporate policies and management processes	**Industry should 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 General Guidelines	
Develop standard	**In collaboration with governments, law enforcement and hotline organisations, industry has a key role to play in combating child sexual abuse content by engaging in the following actions:**	

[6] A “Child”, usually in Europe, is someone under the age of 14-15 years, while “Young people” are those aged 15, 16 and 17. These definitions reflect the OFCOM Broadcasting Code which classifies "Children" as "people under the age of fifteen years", but these terms need to be adapted to national legislations: in Austria, for instance, the right to vote has been recently extended to 16 years old people, while major US Social networks sites fixes the minimum age at 13 years. 'Parental consent' is normally required before involving anyone under 16 in PSB output. However, age may not be the only consideration when COP applies.

processes for handling child sexual abuse content	Refer to General Guidelines	
Develop a safer and age appropriate service environment	**Public Broadcasting Service providers can help to offer a safer, more enjoyable digital environment through the following actions:**	
	The overall parameters, purpose and benchmarks of any project should be discussed with a relevant senior editorial figure. Before a site/profile/page is launched, you should decide what level of engagement you want, what resources you need to achieve it and over what time-frame. Any proposal to use a chat room, message board, microblog or social networking site to find contributors must be referred to the relevant Editor You may put broadcaster branding on a third party site, but the associated content should bring credit to the brand. Advertisements on broadcaster-branded social networking pages should be monitored to check that they are appropriate.	
	It should be clear to users whether a site is a "Broadcaster" page or a "personal" page Broadcasters should not give users the impression that a particular site will have a longer life than is planned. In some circumstances, it may be appropriate to "hand over" a broadcaster page to an online community. You should check online "friends" before approving them and review their comments regularly once approved.	
	Before uploading broadcaster material onto a social networking site, you should make sure that you are aware of, and comfortable with, the site's own terms and conditions. Broadcaster should not seek to duplicate measures of protection and intervention already established by a particular social networking site. There will, however, be times when the broadcaster may implement "light touch" intervention. When forwarding or "retweeting" messages, care should be taken that it does not appear that the broadcaster is endorsing a particular opinion.	
	Broadcaster should be sensitive to the minimum age requirements on different social networking sites. This is often set at 13. Sites aimed at teens should be suitable for that audience. If in doubt, the existing national authorities in charge of child protection may be consulted.	

Empower and educate children, parents, other caregivers, and teachers about children's safety and responsible use of ICTs	**Public Broadcasting Service providers can complement technical measures with education and communication activities through the following actions:**	
	• Prioritise the safety and wellbeing of the child at all times. • Never take sole responsibility for a child; if a child needs care alert the parent or chaperone. • Never give out personal contact details, and do not 'friend' or 'follow' children you are working with on social networking sites. • Never lose sight of the fact that you are with children - behave appropriately and use appropriate language at all times. • Listen to and respect children at all times; don't patronise them. • Always act within professional boundaries; ensure all contact with children is essential to the programme / event / activity / project you are working on. • Ultimately, if you feel anyone is behaving inappropriately around children, you have a duty to report your concern to your local contact at the Broadcaster for child protection.	
Promote digital technology as a mode to further positive civic engagement	**Industry can encourage and empower children's right to participation by:**	
	Refer to General Guidelines	

Content Providers, Online Retailers and Apps Developers

The Internet provides all types of content and activities that are entertaining and educational for children. For instance, online retailers and app providers should build safety and privacy by design into their offerings for young people.

This checklist has been created for content providers, online retailers and app developers that focus on adults and young people.

* This checklist will be discussed further during the Open Consultation.

Content Providers and Retailers Child Online Protection Checklist		Case studies
Identify, prevent, and mitigate the adverse impacts of ICTs on children's rights, and identify opportunities to support children's rights	**Content providers and retailers can help identify, prevent, and mitigate adverse impacts of ICTs by taking the following actions:**	
	Building age-appropriate tools (e.g., tutorials, tools, help centres). • Where relevant, work with online/in-person prevention programs and counselling clinics. For example, an online game site may link an online clinic to help with issues of "addiction," which refers to the way in which some children and young people can become obsessively engaged with technology in such a way as to present an obstacle or a barrier to them developing normal relationships with other people or taking part in healthy physical activities.	
Develop processes for handling child sexual abuse content	**In collaboration with government and law enforcement, content providers can play a key role in combating child sexual abuse content by the following actions:**	
	Ensure that contracts with third parties such as developers, aggregators etc. specifically prohibit illegal content, including child sexual abuse content. • Specify that your organisation will collaborate fully with LE investigations in the event that illegal content is reported / discovered. Also detail any other penalties – e.g. financial fines, revoking of billing privileges. • If your app or service allows customers to upload and store photographs on servers that you own or operate, you should have processes and tools in place to identify images that are most likely to contain child pornography. Such identification processes must be proactive—for example, using a scanning technology or human review.	
	Have processes in place to swiftly remove or block access to illegal	

	content: • Develop Notice and Take Down (NTD)[7] and ensure that third parties with whom your organisation has a contractual relationship have similarly robust NTD processes in place. • Document your practices for handling child pornography, beginning with any monitoring you do and extending to the final transfer and destruction of the content. The documentation should include a list of all personnel responsible for handling the content.	
	It is vital to collaborate with Law Enforcement (LE) / hotline agencies • If your organisation does not yet having working relationships with LE and (if applicable) the national hotline in this area, you will need to engage with them first, and develop processes together.	
	Where possible work with the appropriate functions within your organisation (e.g. customer care, fraud / security) to ensure that you are able to: • Pass on reports of suspected illegal content directly to LE / hotlines– ideally this should be done in such a way that your front line staff are not exposed to the content • Support LE in the event of criminal investigations (e.g. capture evidence)	
	Promote reporting mechanisms for illegal content[8].	
Develop a safer and age appropriate online environment	**Content providers and retailers can help offer a safer, more enjoyable digital environment through the following actions:**	
	Work with reputable 'trusted brand' content providers where possible – especially when dealing with potentially higher risk types of content such as erotic content. Provide a clear external label describing the content on your sites to indicate its suitability for children. Where online content is exactly the same as the "offline" version (e.g. a game or film which differs solely in terms of the access channel), it is possible to re-use existing ratings or classifications. However, where content is new or modified, online content and service providers should find methods of communicating the nature of that content and the target age-range to their customers. If your organization offers audio-visual and multimedia services, the company where applicable may want to provide a specific PIN to users which intend to use adult content or other value added services, whose content can be harmful for children.	

[7] Please see the ISPs checklist for further information

[8] Please refer to the checklist on Mobile Operators for further information

	Ensure transparency in terms of pricing of services and information collected about users. - Ensure your data collection policies comply with relevant law concerning the privacy of minors. Is parental consent required before commercial or other concerns can collect personal information from a child?	
	Supervise the (commercial) content made available online via your service (online forums, social networks, online gaming) - It is vital to adapt your services and content to the user groups that access the services. For instance, if your website is accessed by a very young public, then some necessary changes are needed such as appropriate advertising and data handling policies, content management, etc. - Establish "limits" of online advertising to children.	
	If and where possible adopt appropriate age verification methods to prevent children accessing age-sensitive content, sites or interactive services, such as chat rooms, etc. where risks of inappropriate contact and conduct exist. If your age-classification system relies primarily upon self-certification by your organisation, you will need a clearly defined process for rating content and reporting mechanisms for user to query potentially incorrectly classified content. - Where possible, work together with other industry players to agree on content classification systems that are based on accepted national standards and consistent with approaches taken in equivalent media (e.g. games, film). - Where possible, content classifications from other industries should be re-used. An example might be of a film or film trailer or a PC game (assuming that the images are repeated in the re-purposed for mobile version) so that customers' experiences of the same content are consistent across national media.	
	If the finished content offering also supports an interactive element – e.g. commenting, message boards[9].	
	Communicate in easy to understand, customer-friendly language within your Terms of Service and user guidelines a clear set of "House Rules[10]"	
	Provide advice and reminders about the nature and age-classification of the content they are using.	
	Promote content control options at the point of sale, as part of the set-up process or when the content service is initially accessed. It may	

[9] Please refer to the User Generated Content checklist for additional guidance

[10] Please refer to the Mobile Operators checklist for additional guidance

	be appropriate in some cases to set the default to 'child profile'.	
Empower and educate children, parents, other caregivers, and teachers about children's safety and responsible use of ICTs	**Content providers, online retailers and apps developers can complement technical measures with education and empowerment activities through the following actions:**	
	Display age ratings and describe the nature of the content alongside the description of the content. Research indicates that in general parents want to know about the types of content that may cause concern (such as strong language or violence) rather than being presented with simple age ratings. • To help parents and others decide whether theentertainment content (such as films, videos, DVDs, and computer games) in your service or app is age-appropriate for young players, build your app or service to align with content rating systems: ○ Entertainment Software Ratings Board (ESRB) ○ Pan European Gaming Information (PEGI) ○ International App Rating Council (IARC), which is developing a consistent classification system globally for all apps, particularly for games played on social networks and mobile devices.	
	Tell customers (parents,) what they should know about your services specifically, for example: • What type of content and corresponding parental controls are available; • How to report abuse / misuse / inappropriate or illegal content; • How the complaint report will be handled; • What services are age-restricted; • How to behave safely and responsibly when using built-in interactive services [11].	
	Encourage adults (parents and/or teachers) to be involved in their child's online content consumption, for example: • Accompany younger children so that they can assist and guide their children in the choice of content, as well as help establish appropriate rules of behaviour for them to follow. • Provide rules of use and teach adolescents to be vigilant, well-mannered and responsible while they are navigating the Internet.	
	Industry can encourage and empower children's right to participation by:	

[11] Please refer to the User Generated Content checklist for additional guidance

Promote digital technology as a mode to further positive civic engagement	Develop / offer a range and high quality of rich, compelling, entertaining content that is age-appropriate and, particularly for younger children, encourages / enables them to learn etc. whilst entertaining them and contribute to children's physical, mental and social development providing new opportunities to entertain and educate. Produce content that helps children in education, information, stimulation of imagination and enable new possibilities, in addition to being attractive and usable to them, reliable and safe, and if relevant, make advertising or commercial communication clearly recognizable as such.	

User Generated content/ interactive/social media service providers

If before the online world was dominated mainly by adults, now we are in a world of user-generated content, which is no longer including only adult but also children and adolescents.

In addition, there is no doubt that the explosion of social networking sites has made the issue of controlling user generated content more complex. Social networks are web-wide and young users are potentially open to identity theft, grooming and cyber bullying. In particular, any service which enables users to post and share content with other users to post and share content should expect that its service could be misused by a small minority.

The 'checklist' below has been drafted according to the rules applied by one of the biggest social network This could help other social networks and interactive services who want to develop their COP programme however, it does not mean that all the previsions can be equally applied.

User Generated content / interactive / social media service providers Child Online Protection Checklist		**Case studies**
Develop standard processes for handling child sexual abuse content	**In collaboration with government and law enforcement, UG content / interactive / social media service providers can play a key role in combating child sexual abuse content by the following actions:**	
	Collaborate with Law Enforcement (LE) / hotline agencies in order to effectively handle issues related to illegal content / behaviours, particularly those relating to child sexual abuse content[12]. Work with the appropriate functions within your organisation (e.g. customer care, fraud / security) to ensure that you are able to[13]: • Handle any appropriate messaging to the community and media in response to issues as they arise. This is particularly important where an issue is of public interest and requires prompt attention.	
	Use Terms of Service / Terms and Conditions to specifically prohibit illegal content or behaviours: • Check whether your organisation's ToS / T&C adequately reflect the following: ○ Illegal content, including Child Sexual Abuse Content, will not be tolerated	

[12] Please refer to the Mobile Operators checklist for additional guidance
[13] Please refer to the Finished Content Providers checklist for additional guidance

	○ Your organisation will collaborate fully with law enforcement investigations in the event that illegal content is reported / discovered Adopt appropriate policies regarding the ownership of user generated content, including the option to remove user created content at the user's request.	
	Promote reporting mechanisms for illegal content: • In the event that customers discover child sexual abuse content (or other illegal content), do you have a reporting mechanism you can promote to them? E.g. ○ 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 team(s). ○ Ideally, these teams should be grouped 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 one of these teams. ○ A user's non-compliance with policies for acceptable use may have consequences including removal of content, suspension or closure of their account. E.g., ▪ If the reported piece of content violates the provider's policies, your organization should remove it and warn the person who posted it. ▪ You may also revoke a user's ability to share particular types of content or use certain features, disable a user's account, or refer issues to law enforcement as needed. You also have special teams to handle user appeals for the instances when reports have been filed in error.	
	Have processes in place to swiftly remove or block access to illegal content: • Develop technical systems that either block the creation of illegal content, including in private groups, or flag it for immediate review by your safety team. Create proactive technical measures to analyse the objects and Meta data linked to a profile to detect criminal behaviour or patterns and take actions appropriately. Such developments should be in conformity with public policy on data protection and privacy of the individual. • Develop Notice and Take Down processes[14] .	

[14] Please refer to the Internet Service Providers checklist for additional guidance

	Since the world of interactive and social media providers is a multi-stakeholder community, it is important that your organization establishes relevant partnerships to ensure that you and your customers have relevant information to act on illegal content.	
	Prohibit registered sex offenders: • Social networking sites should ban registered sex offenders from setting up accounts on their sites using technology that already exists today.	
	Cooperate with Law Enforcement: • All sites should have law enforcement hotlines available at all times to assist law enforcement during emergencies and on routine inquiries.	
Develop a safer and age appropriate service environment	**UG content / interactive / social media service providers can help to offer a safer, more enjoyable digital environment through the following actions:**	
	Communicate in a easy to understand, customer-friendly language within your Terms of Service and user guidelines a clear set of "House Rules" for services you offer, which define: • The nature of the service and what is expected of its users • What is and is not acceptable in terms of content / behaviours / language etc. This would prohibit any illegal usage – but this is also an opportunity to ban swearing, bullying, etc. • Consequences of any breach (suspension of account, report tolaw enforcementetc.) • The terms of service should not be a heavy document that will be bypassed during sign up. It is encouraged to make the key messages appear in a relatively simple but unavoidable format during sign up, so that the users are aware of the legalities and acceptable use of terms and conditions while they sign up.	
	Mechanisms for reporting inappropriate content, contact or behaviour should be easily accessible to users at all times[15]. Where applicable, provide age-appropriate content sharing and visibility settings. For example, make privacy and visibility settings for minors more restrictive than the settings for adults by default.	

[15] Please refer to the Internet Service Providers checklist for additional guidance

	Control access to user generated content. Make meaningful efforts to enforce minimum age requirements. • Sites should enforce their minimum age requirements and take steps to identify and remove underage users who have misrepresented their age to gain access. • If your organisation does not yet have in place community age verification systems, you will need to set up appropriate sign-on processes to determine whether users are old enough to access the service. • If appropriate, you can also encourage users to report people who have falsified their age either through the report links on the site or through the dedicated "Help Desk" or "Help Centre".	
	A number of measures may be used to protect online users against inappropriate or illegal user generated content: • Automatic filters—inappropriate words can be blocked from user names and messages at the point of posting. This filter includes swearing, sexual terms, and racist or homophobic language. Non in-house URLs can also be blocked, along with email addresses. In addition wherever possible and appropriate companies should develop tools which allow them actively to seek out and remove content which is in breach of their Ts&Cs. Tools can be develop to prevent the uploading of known illegal content or to detect known illegal content that is already present on the site. • Pre-moderation – message boards can be pre-moderated by a team of specialised 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. • Hosting – In addition to moderators, there can be a team of community hosts who serve as the first point of contact for the moderators when they have concerns about a user.	
	Though password recognition can easily be bypassed, particularly in home environments where the password may be easily identified, these mechanisms are a step in the right direction when it comes to protecting children in gaming and other social media settings. Encourage future biometric and age verification systems through research and development using known international standards and support the development of such tools.	
	Protect for younger users from uninvited communication: • Social networking sites should implement default privacy settings that prevent adults from contacting children under 16 who they do not already know in the physical world. • By default the connection should not be allowed beyond a	

	hierarchy of friends. Nested friend lists should not be allowed for minor profiles.	
	Find ways to review hosted images and videos. • Delete inappropriate ones when found. Tools such as hash scanning and image recognition software are available to assist with this. • Photos and videos should be pre-checked in order to make sure that children do not publish sensitive personal information about themselves or others. In particular, when videos are submitted by children, there is the need for parental consensus.	
	Review discussion groups to find harmful subject matter, hate speech, and illegal behaviour, deleting such content when it is found.	
	Ensure privacy guidelines and how information is collected about users[16].	
	Be responsible for most of the (commercial) content available online (e.g., online forums, social networks, online gaming)[17].	
	Implement appropriate standards and rules to protect children from age inappropriate advertising • Establish clear “limits” for online advertising to children.[18]	
Empower and educate children, parents, other caregivers, and teachers about children’s safety and responsible use of ICTs	**UG content / interactive / social media service providers can complement technical measures through education and empowerment activities through the following actions:**	
	Create a section dedicated to safety tips. • Online users should receive the latest safety information, tips, articles, features, and dialogues about digital citizenship, as well as links to useful content from third-party experts. • Safety and advice should be easily spotted and in easy to use language for children. • The platform providers are also encouraged to make uniform navigation interface across different devices- such as PCs, handhelds and mobile phones	
	Explain to parents the types of content and services now available (e.g. what are social networking sites? What are location-based services? How is the Internet accessed via mobile?) and where relevant, the options available for parents to apply controls.	

[16] Please refer to the Finished Content checklist for additional guidance
[17] Please refer to the User Generated Content checklist for additional guidance
[18] Please refer to the User Generated Content checklist for additional guidance

	Tell parents how to report abuse / misuse / inappropriate or illegal content, and how the report will be handled. • What services are age-restricted. • How to behave safely and responsibly when using built-in interactive services.	
	Establish and promote the importance of social reporting: • This allows people to reach out to other users or trusted friends to help resolve the conflict or open a conversation about a piece of content. • Social reporting is a way for people to quickly and easily ask for help from someone they trust. Safety and child psychology experts state that online issues are frequently a reflection of what is happening offline. By encouraging people to seek help from friends, your organization will find that many of these situations can be resolved face to face. • Social reporting is an especially useful tool, and many people are using it to self-resolve concerns they have about content on the site.	
	Establish a more "trust and reputation" based system to harness good behavior and enable peers to teach best practice to each other by example.	
	Provide advice and reminders about the nature of a given service or content they are using and how to enjoy it safely. For example, build community guidelines into interactive services (e.g. safety pop-ups) reminding users of appropriate and safe behavior – for example, by reminding users not to give out their contact details, and so on.	
Promote digital technology as a mode to further positive civic engagement	**Industry can encourage and empower children's right to participation by:**	
	Refer to General Guidelines	

Hardware Manufacturers

Children and young people today are accessing the Internet using a wide range of electronic devices from laptops to tablets to cell phones and more. Hardware manufacturers can provide built-in technical mechanisms along with education and empowerment activities in order to promote a safe online environment for children and young people.

The 'checklist' below will help those hardware manufacturers who want to develop their COP programme to focus on key areas as a starting point. There is further reading (case studies, additional guidance, etc.) associated with many of the items listed below – this can be accessed by following the relevant links.

* This checklist will be discussed further during the Open Consultation.

Hardware Manufacturers Child Online Protection Checklist		**Case studies**
Develop standard processes for handling child sexual abuse content	**In collaboration with government and law enforcement, hardware manufacturers can play a key role in combating child sexual abuse content by the following actions:**	
	Share information with your customers/ users regarding the applicable legal framework for the online protection of children, under which your organization is operating. [This framework should also be reflected on your organization's relevant policies.]	
Develop a safer and age appropriate service environment	**Hardware manufacturers can help to offer a safer, more enjoyable digital environment through the following actions:**	
	Use Terms and Conditions to draw users' attention to the availability of content found in their online services (App Stores), that may be deemed inappropriate, either originating from the manufacturers themselves or from any other Third-party.	
	Offer easy-to-use parental control options, which allow parents to restrict the services and content that children can access when using the several electronic devices. These restrictions can include: • access to social media; • internet access; • application/game purchase and installation; • use of location services. When turning on Parental Controls a PIN is required to change the allowed services, which prevents children or other parties from changing your settings.	
Empower and educate children, parents, other caregivers, and	**Hardware manufacturers can complement technical measures with education and empowerment activities through the following actions:**	
	• Support customers by making available useful guidelines for family online safety, encouraging parents	

teachers about children's safety and responsible use of ICTs	to: ensure a moderate use of electronic devices and services by their children as part of an otherwise healthy and balanced lifestyle; • Get familiarized with the services and products their children are using; • Pay close attention to the behaviour of their children in order to identify possible changes which could be linked to online bullying or harassment; • Become aware of the physical risks imposed on children by the excessive use of the respective electronic devices.	
Promote digital technology as a mode to further positive civic engagement	**Industry can encourage and facilitate children's right to participation by:**	
	Refer to General Guidelines	

CONSULTATION QUESTIONNAIRE

Kindly type your responses directly into the text boxes provided.

PARTICIPANT INFORMATION

1. Please tell us about yourself. Alternatively, you may provide your input anonymously.

2. In what capacity are you responding?

Personal
Professional / Official

3. Input provided will not be publicly attributed to any organization or individual. However, please indicate if we may disclose the fact that you or your organization provided input in the process.

Yes
No

4. Which sector do you belong to? Please check one box.

Private Sector / Business*
Civil Society
Academia
Non-Governmental Organization
Trade Union
Government
United Nations
Other, please specify:
*For Private Sector/Business and ICT, can you please provide your sub-sector

5. May we add your contact information to our "Interested persons" list to keep you informed about the process related to the development of the Guidelines and/or in the event we need to contact you to clarify your responses?

Yes
No

A. ASSESSING THE COVERAGE AND CONTENT OF THE DRAFT GUIDELINES

6. Please comment on the *scope* of the draft Guidelines. Are there topics covered that should not be, or are there gaps?

I agree with the scope of the Guidelines – they cover all the pertinent themes.
I don't agree with the scope of the Guidelines.

7. Please explain or provide other comments on the scope/coverage of the draft Guidelines:

8. Please comment on the *content* of the draft Guidelines, including any suggestions for redrafting of particular provisions. Use additional space as needed.

9. Should the Guidelines distinguish more clearly between must dos and nice to haves?

Yes
No

If so, how?

B. CONSIDERATIONS ON APPLYING THE GUIDELINES

10. Please share one or more examples of a policy, practice or initiative your organization is involved in that is relevant to the draft Guidelines and the topic of child online security and ICTs (links to existing material are fine). (The partner organizations may draw on this material for good practice examples of how to implement the Guidelines).

11. How might the Guidelines be helpful to you and your organization?

12. What would be helpful to include in commentary and documentation that accompanies the final version of the Guidelines? (Select all that apply)

Case Studies / Good Practice Examples
The business case for the Guidelines
Assessment tools to measure progress
Facts & Figures
Glossary of Terms
Other, please specify:

C. THOUGHTS ON NEXT STEPS

15. Once the Guidelines are finalized, what steps should be taken with regard to these Guidelines? (Select all that apply):

Collect and share resources/guidance materials and tools that may help businesses/organizations with their application of the Guidelines
Collect and share good practice examples illustrating action businesses/organizations can take to help with their application of the Guidelines
Work with others to fill gaps in guidance on specific issues relating to ICTs and children (please specify any needs below)
Create an initiative around the Guidelines and their implementation

Please elaborate or indicate any other recommendations here:

D. ADDITIONAL COMMENTS AND/OR QUESTIONS Please limit your input to 500 words.

18. If you have additional comments, kindly indicate them below.