Ministry of Post and Telecommunications

CAMBODIAN CHILD ONLINE PROTECTION GUIDELINES FOR THE DIGITAL TECHNOLOGY INDUSTRY

Full Report 2023

unicef
for every child

End Violence Against Children

CONTENTS

FOREWORD

The Ministry of Post and Telecommunications (MPTC) has established the "Cambodian Child Online Protection Guidelines for the Digital Technology Industry" to address the growing concerns about child online risks and harms. The Guidelines aim to encourage the industry to take preemptive and effective actions to ensure that their products and services are safe for young users in Cambodia, with timely response in case any harms arise.

Digital technologies are a potential catalyst in the development of Cambodia and provide benefits to the public, including children. Current statistics on Internet usage indicate that one out of three users is a child. The COVID-19 pandemic has accelerated this trend as digital technologies have become essential tools for children to communicate, research, and pursue their education. This trend will continue as the Royal Government of Cambodia (RGC) has adopted the Digital Economy and Society Policy Framework 2021-2035 and Digital Government Policy 2022-2035 in response to the 4th Industrial Revolution and in pursuance of the digital transformation vision for Cambodia. These policy reflect the RGC's long-term strategies to digitalize all sectors, including the government, businesses, and citizens. The goal is to enhance economic growth, improve social well-being, and deliver efficient and effective public services. On this note, individuals including children are encouraged to make use of and incorporate digital technologies into their daily lives as a good digital citizen. Therefore, ensuring digital safety and well-being has become a priority for the successful digital transformation of Cambodian society.

Of all Internet users, children are the most vulnerable group. Therefore, the 2021 General Comment No. 25 of the UN Committee on the Rights of the Child (CRC) highlights the importance of the digital environment for children's livelihoods and rights. While online, children are at risk of child online abuse and sexual exploitation, cyberbullying, online grooming, child sexual abuse material (CSAM), and acceptance of negative behaviors, to name a few. The aforementioned risks could be prevented and mitigated given the collaboration and cooperation among government institutions, regulators, parents and/or guardians, educators, NGOs, industry, and children themselves. The Ministry of Post and Telecommunications, responsible for advancing the country's digital development; hence, has established technical guidelines aligned with national and international standards. These guidelines

aim to ensure that the digital products and services of the private sector are user-centric and friendly, particularly in strict adherence to children rights and business ethics. Nonetheless, the active collaboration and engagement of all relevant stakeholders are essential for the successful implementation of these guidelines.

The development of these guidelines would not have been possible without the support and contribution of the Global Partnership to End Violence Against Children, UNICEF Cambodia, line ministries, industries, and relevant stakeholders. I would also like to thank the MPTC technical working group their hard work and dedication to prepare this document until its finalization. I highly encourage private companies to take note of and comply with these Guidelines to safeguard the safety and well-being of our children in this digital age. Ensuring a risk-free digital environment for children is our collective responsibility that each of us shares.

Phnom Penh, 29th June 2023

Minister of Post and Telecommunications

CHEA Vandeth

LIST OF ACRONYMS

AI	Artificial Intelligence
API	Application Programming Interface
ASEAN	Association of Southeast Asian Nations
COP	Child Online Protection
CRBP	Children's Rights and Business Principles
CNCC	Cambodian National Council for Children
CRC	(United Nations) Convention on the Rights of the Child
CRIA	Child Rights Impact Assessment
CSAM	Child Sexual Abuse Material
MoEYS	Ministry of Education, Youth and Sport
MoH	Ministry of Health
MPTC	Ministry of Post and Telecommunication
MoI	Ministry of Interior
MoSVY	Ministry of Social Affairs, Veterans and Youth Rehabilitation

MoWA	Ministry of Women's Affairs
OCSEA	Online Child Sexual Exploitation and Abuse
ICT	Information and Communication Technology
ICSE	International Child Sexual Exploitation Image Database
ICMEC	International Center for Missing and Exploited Children
IoT	Internet of Things
ILO	International labour Organization
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunications Union
IWF	Internet Watch Foundation
MNR	Model National Response
UNGPs	United National Guiding Principles on Business and Human Rights
UNICEF	United Nations Children's Fund
URL	Uniform Resource Locator (web address)
VAS	Value-Added Services
WHO	World Health Organization

GLOSSARY OF TERMS

Term	Definition
Age-Appropriate Design	The consideration of the age of the end-user of a product or service and the evolving capacities and developmental stages of a child, and associated risks, into the design and development of any new product or service. This ensures that from the outset of a product/service development, the impact of that product or service on children of different ages is considered and reflects children's agency and evolving capacities in a way that do not put children's well-being and rights at risk. Being age-appropriate also means offering opportunities for growth and development in ways that are compatible with children's developmental requirements.
Age-verification *From: Explanatory Notes to the UK Online Safety Bill (drafted dated 17 March 2022), Bill 285- EN, para. 381.*	Age assurance measures are technical measures used to restrict access to age-inappropriate content (this should be used together with the age-appropriate guidelines attached as an Appendix to this document)
Artificial Intelligence *ITU. Guidelines for industry on Child Online Protection, 2020*	In the broadest sense, artificial intelligence (AI) refers indistinctly to systems that are pure science fiction (so-called "strong" AIs with a self-aware form) and systems that are already operational and capable of performing very complex tasks (systems described as "weak" or "moderate" AIs, such as face or voice recognition, and vehicle driving).
Child *Draft Law on Child Protection, 2022; also, CRC*	Any person under the age of 18

Child Safeguarding

Child safeguarding refers to a set of policies, processes and practices designed to actively prevent harm or distress to children. Safeguarding is specifically focused on preventative actions to ensure that children are protected from deliberate or unintentional acts that may lead to the risk of or actual harm.

Child sexual exploitation and abuse

Article 18, Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)

ECPAT Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Adopted by the Interagency Working Group in Luxembourg, 28 January 2016

See also: Committee on the Rights of the Child, Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/156, 10 September 2019

Child sexual abuse includes:

(a) Engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities (this does not apply to consensual sexual activities between minors), and

(b) engaging in sexual activities with a child where use is made of coercion, force or threats; or abuse is made of a recognized position of trust, authority or influence over the child, including within the family; or abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.

Child sexual abuse becomes sexual exploitation when a second party benefits monetarily, through sexual activity involving a child. It includes harmful acts such as sexual solicitation and sexual exploitation of a child or adolescent in prostitution and, in the Council of Europe Convention, covers situations in which a child or other person is given or promised money or other form of remuneration, payment or consideration in return for the child engaging in sexual activity, even if the payment/ remuneration is not made.

Although the terms are sometimes used interchangeably, what distinguishes the concept of child sexual exploitation from child sexual abuse is the underlying notion of exchange.

Child sexual abuse material (CSAM) *Committee on the Rights of the Child, Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/156, 10 September 2019, para 60.* *Also, Draft Law on Child Protection, Kingdom of Cambodia*	Child sexual abuse material is covered under article 2 of the Optional Protocol to the CRC on the sale of children, child prostitution and child pornography as 'child pornography', and is defined 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 (art. 2 (c)) The Committee on the Rights of the Child recommends that States' parties, in line with recent developments, avoid the term 'child pornography' to the extent possible and use other terms such as the 'use of children in pornographic performances and materials', 'child sexual abuse material' and 'child sexual exploitation material'.
Cyberflashing	The unsolicited sending of images (including video) of genitals with the use of digital technologies.
Cyberbullying	Cyberbullying describes an intentionally aggressive act carried out repeatedly by either a group or an individual using digital technology and targeting a victim who cannot easily defend him or herself. It usually involves "using digital technology and the internet to post hurtful information about someone, purposely sharing private information, photos or videos in a hurtful way, sending threatening or insulting messages (via email, instant messaging, chat or texts), spreading rumours and false information about the victim or purposely excluding them from online communications". Increasingly, acts are considered cyberbullying even if they are not repetitive, but if all other factors are present.
Cyberhate, discrimination and extremism	Cyberhate, discrimination and violent extremism are a distinct form of cyber violence as they target a collective identity, rather than individuals, … often pertaining to race, sexual orientation, religion, nationality or immigration status, sex/gender and politics".

Digital Education	Any teaching or learning processes that entail the use of digital technology, including online and offline formats, using distance, in-person, or hybrid approaches.
Doxing	The act of publicly disclosing private information, usually online, about an individual. This could include addresses and locations, age, work or employment details, sexual orientation, or any other personal identification data.
Education technology (EdTech)	The practice of using technology to support teaching and the effective day-to-day management of education institutions. It includes hardware (such as tablets, laptops or other digital devices), and digital resources (such as platforms and content), software and services that aid teaching, meet specific needs, and help the daily running of education institutions.
Helpline	Helplines provide advice (usually with the option of confidentiality) and assistance to callers, often acting as points of referral to other service providers.
Hotline	A dedicated online reporting mechanism to report Internet material suspected to be illegal, including child sexual abuse material. A hotline enables the public to anonymously report online material they suspect may be illegal. A Hotline is distinct from a Helpline (see above).
(Technology-facilitated) Image- Based Sexual Abuse	The non-consensual creation and/or distribution and/or threat of distribution of private, sexual images. Image-based sexual abuse may be used to describe a range of non-consensual offences involving the creation and dissemination of private sexual images, including what was previously know as "revenge pornography." It also includes image-based sexual harassment, which refers to the unsolicited sharing of sexual images. A distinction must be made between image-based sexual abuse and sexting. The former constitutes a form of abuse, while sexting is a consensual act between two (or more) parties.

Livestreaming of Child Sexual Abuse and Exploitation

From United Nations Children's Fund (2021) Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries, UNICEF, New York;

From the ASEAN Regional Plan of Action for the Protection of Children from all forms of Online Child Sexual Exploitation and Abuse, 2020

Transmitting child sexual abuse and exploitation in real-time over the internet. This occurs on online chat rooms, social media platforms, and communication apps with video chat features. Viewers of livestreaming child sexual abuse can be passive (pay to watch) or active by communicating with the child, the sexual abuser and/ or facilitator of the child sexual abuse, and requesting specific physical acts. Another form of livestreaming can involve coercing a child to produce and transmit sexual material in real-time.

The ASEAN Regional Plan of Action defined Livestreaming as child sexual exploitation and abuse (CSEA) carried out in real-time and viewed through streaming (and sometimes recorded) the content online, while the victim and perpetrator are in different or in the same countries.

While live streaming can be an intentional method used by perpetrators to minimize digital evidence of their crime, these interactions can also be recorded, thereby generating new CSAM that can be further shared online. In many cases, payment is exchanged and perpetrators often have the chance to direct the abuse of the child via the facilitator. Payment is generally made using a variety of online payment methods, including cryptocurrencies.

Notice and Takedown orders

Adapted from United Nations Children's Fund (2021) MO-CRIA:

Child Rights Impact Self-assessment Tool for Mobile Operators, UNICEF, New York

Notice and Takedown orders are notification and instructions issued by Law Enforcement Agency (or in some countries) a recognized CSAM Hotline, to a national or international hosting provider (for example ISP, social media company or search engine) of CSAM content and for the removal (Takedown) of such content as soon as it has been informed of such content (Notice)

Online child sexual exploitation and abuse

Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Adopted by the Interagency Working Group in Luxembourg, 28 January 2016

See also: Committee on the Rights of the Child, Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/156, 10 September 2019, and

ASEAN Regional Plan of Action for the Protection of Children from all forms of Online Child Sexual Exploitation and Abuse, 2020

Often used interchangeably with 'technology-facilitated child sexual exploitation and abuse' to refer to child sexual exploitation and abuse that is partly or entirely facilitated by technology, that is the internet or other wireless communications.

For example, child sexual abuse takes on an online dimension when, for instance, acts of sexual abuse are photographed or video-/audio recorded and then uploaded and made available online, whether for personal use or for sharing with others. Each repeated viewing and/or sharing of such recorded material constitutes a new violation of the rights of the child.

The ASEAN Regional Plan of Action for the protection of children from all forms of online child sexual exploitation and abuse locates its definition in the above, and described OCSEA as "any use of information and communication technologies (ICTs) that results in sexual exploitation or causes a child to be sexually exploited or that results in or causes images or other material documenting such sexual exploitation to be produced, bought, sold, possessed, distributed, or transmitted. OCSEA includes grooming, indecent images of children taken through coercion, threats, force, deception or persuasion or through peer-to-peer sharing, and use of children in audio or visual images of child abuse."

Parental control tools

UNICEF, 2021, MO-CRIA: Child Rights Impact Assessment Tool for Mobile Operators (2nd Edition)

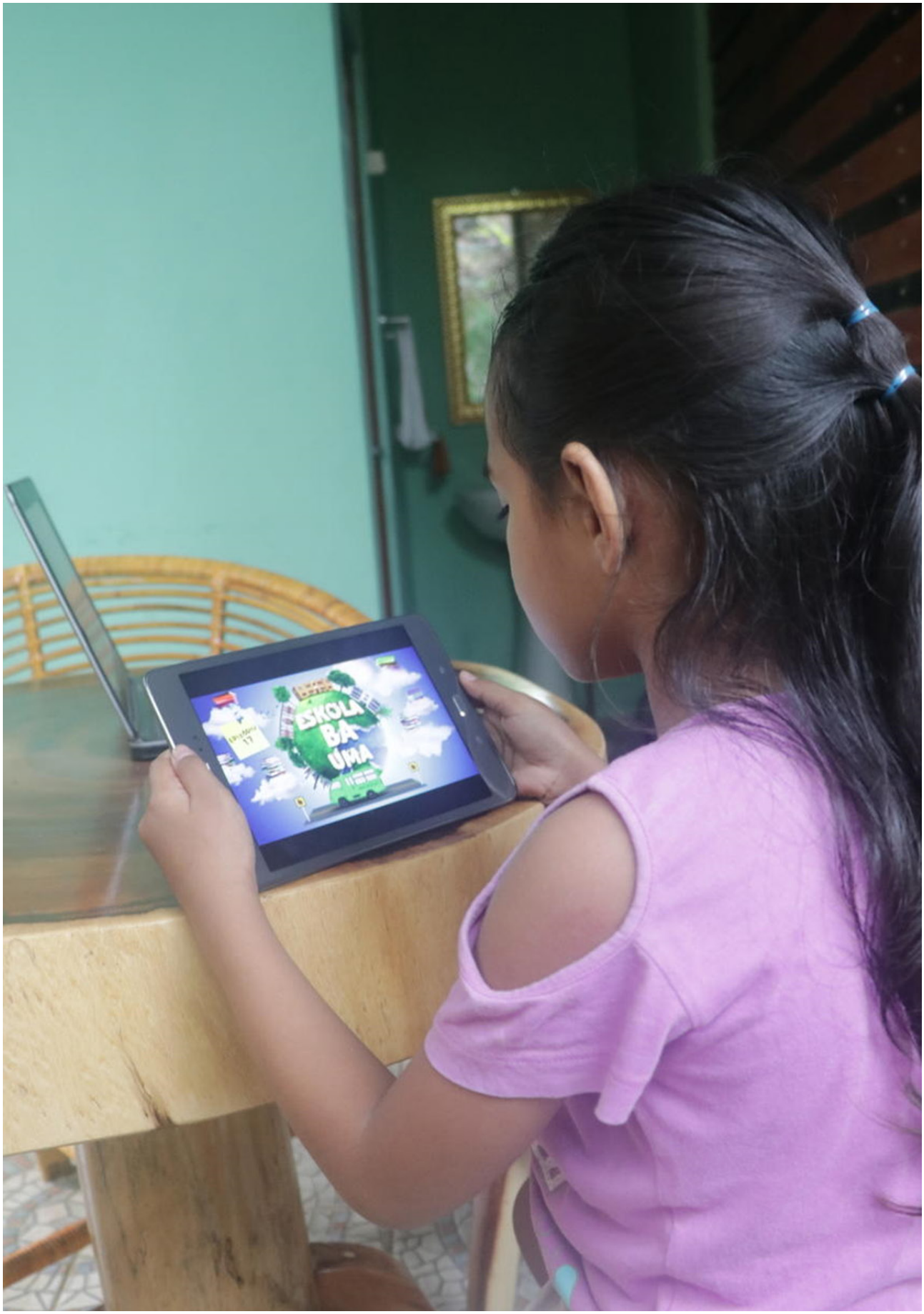
Software that allows users, typically a parent, to control some or all functions of a computer or other device that can connect to the internet. Typically, such programmes can limit access to particular types or classes of websites or online services. Some also provide scope for time management, e.g. 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.

Control tools need to strike a balance between the right to protection from all forms of violence and exploitation, and a user's rights to information, freedom of expression, privacy and non-discrimination, as defined in the CRC. It is unlikely to be possible to remove all the risks to children that exist online. Additionally, beyond a certain point, attempting to do so could threaten children's access to the multiple benefits provided by meaningful access to the internet.

Personal data *General Data Protection Regulations,*	*Any information relating to an identified or identifiable natural person (data subject)*
Prevention *World Health Organization (WHO), World Report on Violence and Health, WHO, Geneva, 2002.*	Follows the WHO definition of 'primary prevention': Stopping child sexual abuse and exploitation before it occurs.
Privacy-by-design	The planning and integration of privacy mechanisms into any app, software or product from the conceptualization through to design and development stages of production, thus ensuring that the privacy rights and needs of children are fully integrated into products from the start.
Reporting Portal	A customized webpage, mobile app or in-app mechanism where people can report suspected child sexual abuse material.
Safety-by-design	The planning and integration of safety mechanisms into any app, software or product from the conceptualization through to design and development stages of production, thus ensuring that the safety and protection rights and needs of children are fully integrated into products from the start.
Sexting	The sending or receiving of sexually explicit or sexually suggestive images or video or text. Sexting usually refers to consensual behaviour between two or more parties but may escalate to image-based sexual abuse or other OCSEA if images, videos or messages are posted, shared without both parties' explicit consent, or if any form of coercion is introduced. Sexting between any adult and a child who has not yet reached the age of consent should be treated as an offence. Exceptions may be made where the act is consensual between a minor and an adult with no more than two years difference in age. Care should be taken, as per guidance from the CRC, not to criminalize consensual sexting between two children.

Sexual Extortion, or Sextortion of a child *From the ASEAN Regional Plan of Action for the Protection of Children from all forms of Online Child Sexual Exploitation and Abuse, 2020* *Also Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Adopted by the Interagency Working Group in Luxembourg, 28 January 2016*	The blackmailing of a child with the help of images of that child, including self-generated images of that child in order to extort sexual favours, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted child (e.g. posting images on social media). Sexual Extortion is the preferred term, as sextortion may not convey the seriousness and exploitative nature of this act.
Sexual violence *Based on definition in Krug et al. 2002, op. cit. (see Child Maltreatment).*	An umbrella term used here to refer to all forms of sexual victimization of adults and of children – child sexual abuse and exploitation, rape and other sexual assaults, sexual harassment, abuse in pornography, prostitution and trafficking, or FGM. Any sexual act, attempt to obtain a sexual act, unwanted sexual comments or advances, or acts to traffic, or otherwise directed at a person's sexuality using coercion, by any person, regardless of their relationship to the victim, in any setting, including but not limited to home and work.

(Digital) Digital technology industry *ITU. Guidelines for industry on Child Online Protection, 2020*	The Digital technology sector (also ICT or Information and Communication Technology) covers a broad range of companies including but not limited to: (a) Internet Service Providers (ISPs), including through fixed landline broadband services or cellular data services of mobile network operators: while this typically reflects services offered over a more long-term basis to subscribed customers, it could also be extended to businesses that provide free or paid public WI-FI hotspots. (b) Mobile Network Operators (may also serve as ISPs). (c) Social network /messaging platforms and online gaming platforms. (c) Hardware and software manufacturers, such as providers of handheld devices including mobile phones, gaming consoles, voice assistance-based home devices, Internet of Things and smart Internet connected toys for children. (d) Companies providing digital media (content creators, providing access to or hosting content). (e) Companies providing streaming services, including live streams. (f) Companies offering digital file storage services, cloud-based service providers.
Violence against children *Article 19, Convention on the Rights of the Child (CRC), 1989*	All forms of physical or psychological violence, injury and abuse, neglect or negligent treatment, maltreatment or exploitation, including emotional violence and sexual abuse.


ASKOLA
BA
UMA

INTRODUCTION

"The rights of every child must be respected, protected and fulfilled in the digital environment. Innovations in digital technology affect children's lives and their rights in ways that are wide-ranging and interdependent" (United Nations Committee on the Rights of the Child).[1]

Digital technology, including the internet has fundamentally changed how people the world over live their life every day. Even those who may not directly have access to the internet themselves may find themselves impacted in different and meaningful ways by digital technology. No single one section of society has been more affected by these changes than children, particularly in recent years through the COVID-19 pandemic, as children integrate technology into their lives at an unprecedented rate. For months, and sometimes years, children's entire life, from learning to communication with friends and extended family, to play, moved into the digital space. This process clearly illustrates the benefits and opportunities that digital technology can bring to children's lives. At the same time, it is now well-documented that access to and use of digital technology may provide an additional space in which children can encounter varied risks, that may result in harm to children's wellbeing, rights and safety.

In Cambodia, 36% of the total population are below the age of 18.[2] This means that 6,051,000 of current or potential internet users are under the age of 18. While at a population level, internet subscription or penetration rates are at 40.5%,[3] recent data shows that more than four out of five children between the ages of 12 and 17 have access to the internet, with nine in ten children between the ages of 16- and 17-years having access to the internet.[4] That means that the majority of children in Cambodia are going online in different ways, using different devices and platforms and apps, all of which may impact their lives in different ways, and which may, if not appropriately designed, managed and operated, present children with substantial risk of harms. The digital technology industry in Cambodia thus has a critical role to play in ensuring that every reasonable step is taken to keep children safe when online and using digital technology, including AI or machine-learning devices, and to respond quickly and efficiently when children are placed at risk.

These Cambodian Child Online Protection Guidelines for the Digital Technology Industry have been developed following the analysis conducted by the Ministry of Post and Telecommunication on the readiness of the digital technology industry in Cambodia to prevent and respond to online child

[1] United Nations Committee on the Rights of the Child. (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment. CEC/C/GC/25. 2 March 2021. Para 4.

[2] United Nations (2021). The State of the Worlds Children 2021. UNICEF. New York.

[3] International Telecommunications Union. (2020). Country ICT data: Percentage of Individuals Using the Internet.

[4] ECPAT, INTERPOL and UNICEF. (2022). Disrupting Harm in Cambodia: Evidence on Online Child Sexual Exploitation and Abuse. Global Partnership to End Violence Against Children.

sexual exploitation and other forms of violence against children.[5] The need for these Guidelines was identified within the Cambodian National Council for Children's Initial Situational Analysis on Online Child Sexual Exploitation (OCSEA) in Cambodia, as well as the Disrupting Harms Cambodia Study[6], and is embedded in the National Action Plan to Prevent and Respond to Online Child Sexual Exploitation in Cambodia 2021-2025. The Guidelines are also consistent and aligned with the 2021 Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN. While these Guidelines are intended primarily for the Cambodian digital technology sector, they are consistent with, and informed by, the laws and regulations that govern most of the international social media companies, although the policies and processes of these companies largely fall outside of the legal jurisdiction of the Cambodian Government.

Child Online Protection is a complex challenge, that requires the commitment and efficient coordination and functioning of different actors both within the private sector, and within the Government. Within the Cambodian government, the Cambodian National Centre for Children (CNCC) assumes the role for the coordination of the implementation of the OCSEA Action Plan, working closely with different government partners, civil society and industry. Within government, the MPTC is the lead agency responsible for private sector engagement relating to COP, while the Ministry of Social Affairs, Veterans and Youth Rehabilitation (MoSVY); Ministry of Education, Youth and Sport (MoEYS)s; Ministry of Women's Affairs (MoWA); Ministry of Justice (MoJ); Ministry of Health and Ministry of Interior (including the National Police and Cyber Crime Unit) all have important roles. Similarly, within the private sector, all those within the digital technology industry have a role to play. While much of the focus often falls on the role of social media companies in addressing child online protection, ISPs, Mobile Operators, data hosting companies, content creators and producers and software and App developers all have an explicit role to play in ensuring that children are safe online, and that all their rights are respected. The recent UNICEF Global Guide on Legislating to prevent Online Child Sexual Exploitation[7] details the 'internet value chain' and provides an overview of five categories of services within the industry. Each of these, well-represented within the Cambodian digital technology industry, have an explicit role to play in keeping children safe online and in protecting children's rights in the digital environment.

What is Child (Online) Protection?

Child protection broadly refers to the prevention and response to violence, exploitation and abuse against children in all situations and contexts. Child Online Protection refers to the prevention and response to all forms of violence, abuse and exploitation within the digital space, while recognizing that what happens online is rarely confined to the digital space, but rather, is deeply connected to what happens offline. Rather, the digital space is just one context in which violence can occur, which may be facilitated through the use of technology.

[5] Ministry of Post and Telecommunications (2022). Child Online Protection within the Cambodian Digital technology industry: Assessment report. Unpublished research report

[6] Kardefelt Winther, Daniel (2022). Disrupting Harm in Cambodia: Evidence on online child sexual exploitation and abuse, Innocenti Research Report, UNICEF Office of Research - Innocenti, Florence

[7] United Nations Children's Fund (2022) 'Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse' UNICEF, New York.

Table 1. Unpacking the digital technology industry – the internet value chain[8]

Content Rights	Companies that own, and in most cases sell to others, the rights to various types of content for distribution via the Internet. These could include professionally produced content, available with or without premiums, or professionally produced or amateur-produced user-generated content.
Online services[9]	Online services consist of a diverse range of consumer and business services provided over the internet through browsers or application platforms. These include e-commerce services; entertainment services (including gaming, video and music services; search engines; social and community platforms; and cloud and other e-services.
Enabling technology and services	Consist of a wide range of services that often are not immediately visible to Internet users but are essential to the efficient operation of the overall Internet infrastructure and the websites, servers, platforms, and services that use it.
Connectivity	Suppliers of services, such as broadband, 2G, 3G or 4G data services, which connect end users to the internet via mobile or fixed access.
User Interfaces	Includes the devices, systems, and software used by end users to access the internet and services outlined above.

[8] Adapted from United Nations Children's Fund (2022) 'Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse' UNICEF, New York.; and GSMA, The Internet Value Chain: A study on the economics of the internet, May 2016, <www.gsma.com/publicpolicy/wp-content/ uploads/2016/09/GSMA2016_Report_TheInternetValueChain.pdf>, accessed 1 December 2021, p. 15.

[9] According to GSMA, this category probably covers most of what people think of as "the internet". P15

BOX: Children Online in Cambodia

Children in Cambodia are veracious users of digital technology. 8 in 10 children aged at 12 to 17 are internet users, with no difference between boys and girls. Like many other countries, children tend to use the internet more than their parents, which has implications for the degree to which parents and caregivers can provide guidance or support to their children on their online activities. Almost four in five children use the internet at least once a day, while only 42% of parents or caregivers access the internet at least once a day.

Children most commonly use their smartphones to go online (99%), and many share their phones with someone else. The most common activities reported by children in Cambodia were entertainment-related, with 79% reporting that they watch videos and use social media, respectively. All children included in the study who used the internet accessed the internet from home, with one in three also accessing the internet at school, and 14% at an internet café.

Children frequently report engaging in risky behaviour online, including meeting someone in person they had first met online or sharing naked images or videos of themselves (both 9% of children). These behaviours did not commonly result in harm to the children, although when they did, the harm experienced was severe. More than 1 in 10 children (11%) had experienced some form of online child sexual exploitation or abuse, including sexual exploitation, sharing of their sexual images or video without permission, or coercive sexual activities. These experiences of abuse had primarily occurred on Facebook Messenger and the Facebook platform, TikTok, and YouTube.

Importantly, most experiences of OCSEA are not reported or disclosed through formal reporting systems, limiting the chance of a systemic and institutional response, and the provision of adequate services.

The recent Disrupting Harms study noted several recommendations that directly impact industry, including the imposition and enforcement of regulatory and criminal penalties on companies not acting to prevent and respond to CSAM, as well as ensuring companies make reporting and blocking mechanisms in platforms visible and easy to use, and implement standards to actively remove inappropriate content.

Source: Kardefelt Winther, Daniel (2022). Disrupting Harm in Cambodia: Evidence on online child sexual exploitation and abuse, Innocenti Research Report, UNICEF Office of Research - Innocenti, Florence

Intention of these Guidelines

- The adoption of these standard industry guidelines for Cambodia will create a level playing field for all digital technology companies in Cambodia, assuming adherence to the guidelines, to ensure that no company is placed at a comparative disadvantage.
- They will ensure a uniform and consistent approach to addressing the risks that children face online, and minimizing harms, in a way that respects the collective rights of children in the digital environment, and that integrates the best interests of children.
- They will establish an integrated approach that allows seamless coordination of all those actors who are necessary to prevent and respond to all forms of violence online, including OCSEA.
- They will ensure alignment of Cambodian digital technology companies with global, regional and national models and frameworks of best practice.

These Guidelines have been drafted for all digital technology companies and enterprises in Cambodia, both Cambodian businesses and international companies who's products and services are delivered and used in Cambodia. This is a particularly important consideration given the global nature of digital technology and the internet.

These Guidelines have been written to be consistent with, and reflect, global guidance, and as such, should largely reflect the operating modalities of the global digital technology industry. However, in all matters relating to the provision and delivery of digital technology services and products within Cambodia, Cambodian laws and regulations apply, regardless of where businesses are domiciled.

These Guidelines, while not legally binding, provide a critical common commitment by the digital technology industry in Cambodia to proactively addressing the safety and wellbeing of children online, from a child-rights perspective. They should be seen as complimentary to the laws and regulations of Cambodia relating to the protection and safety of children, reflecting regional and global obligations to act, regulate and provide oversight of the digital technology in respect to children's rights, including the prevention of OCSEA and other forms of technology-facilitated violence. This includes the regulation of industry to ensure the protection of children's collective rights in the digital environment, ensuring industry takes proactive and transparent steps to address OCSEA, and to do no harm to children. Various aspects of these are contained in existing and pending legislation and policies, such as the draft Cyber Crime Bill. The Guidelines can serve as an important resource to bind the digital technology sector in Cambodia, and global companies operating within Cambodia, to a common approach to addressing Child Online Protection, in conjunction with national laws and regulation of the industry, to collectively achieve a common goal. There is increasing recognition that a combination of regulation and self-regulation of the digital technology is the most effective to ensuring a coordinated, equitable and effective mechanism to ensure the protection of children in the digital environment, in a way that fully respects and enshrines the effective rights of children as they translate fully into the digital space.

Structure of the Guidelines

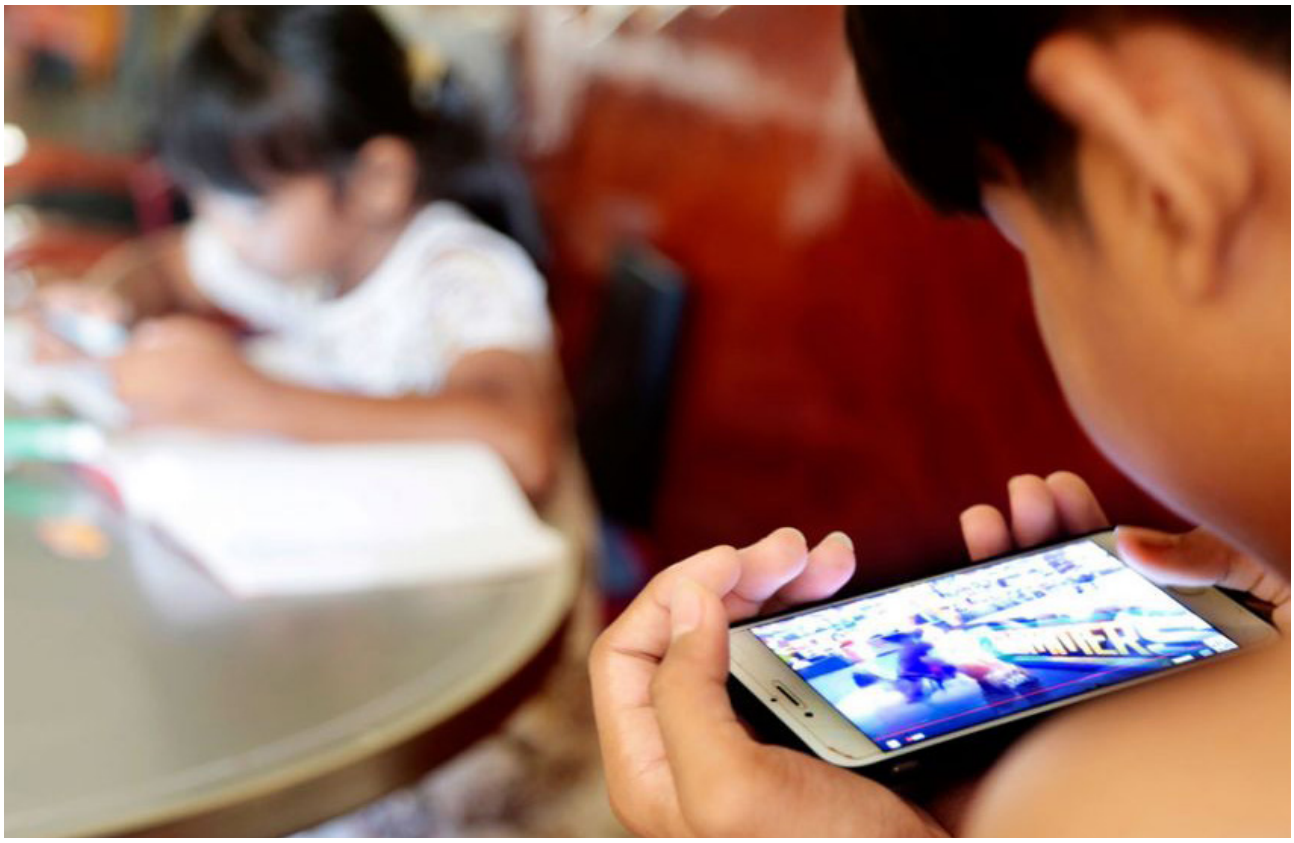
These guidelines contain three sections: they first provide an introduction to child rights in the digital environment, in the section Child Rights and Child Online Protection for the Digital Technology Sector, within which all actions by industry to protect children online should be framed. This section also provides a brief introduction to some of the most pressing safety concerns for children.

The second section, Applying Global and Regional COP frameworks to the digital technology sector in Cambodia, locates the work of the digital technology industry in Cambodia within the main child and human rights global and regional frameworks on ending violence against children and online sexual violence against children, as well as the Child Rights and Business Principles (CRBPs).

The third section, Practical COP Mechanisms for the Cambodian Industry, provides the practical steps that the digital technology industry in Cambodia should take in its efforts to ensure an equitable, comprehensive, evidence-led, and effective approach to child online protection.

Each section is prefaced with a Section Snapshot. This section provides a very quick summary of some of the main points contained in the following section. These summaries should not be read as a full synthesis of the section and are in themselves insufficient for the reader to gain a full appreciation of the complexities and expectations contained in the full chapters.

The Appendices contain an overview of further global frameworks of use, and a categorization by age and developmental stage of children's technology use, as well as a Checklist that companies can use to assess their COP processes and responsibilities, and that can be used by the MPTC to evaluate companies compliance with the Guidelines.



When children from Cambodia, Thailand, Indonesia, Malaysia, Myanmar, Philippines and Viet Nam were asked about what they want the technology private sector to do to keep them safe online, they asked for the private sector to ***"put children's needs, vulnerabilities and contexts at the heart of the design of all products and services".***

UNICEF East Asia and Pacific Regional Office/Western Sydney University, A call to action from children and young people to the private sector on child online protection, Bangkok 2022.

WHY THE DIGITAL TECHNOLOGY INDUSTRY SHOULD CARE ABOUT CHILD RIGHTS

SECTION SNAPSHOT:

- The digital technology industry in Cambodia has an important role to play in keeping children safe online within a framework on children's rights.
- Companies should undertake Child Rights Impact Assessments as the departure point to inform their actions to ensure that children's rights, including to protection and privacy, are respected and enshrined in all areas of their business, and are integrated into all products, services or activities.
- Steps that that technology companies take to keep children safe should not infringe on children's other rights, including but not limited to their right to information, privacy, freedom of expression, personal data protection, education, or to play, including through digital technology and the internet.
- Industry from always thinking and planning for the consideration that children may use their products or their services, and how their products, from the design to the delivery stage, might impact on children of different age groups and abilities.
- Digital technology companies in Cambodia must always consider how their products and services may advantage some children and disadvantage others and strive to promote equitable access for all children.
- When considering how to keep children using their products and services, or who may be exposed to them, safe in the digital environment, technology companies in Cambodia must consider the wide range of risks that children may encounter online: contact risks, content risks, conduct risks, and contract risks. They must also consider ALL forms of technology-facilitated violence that children encounter.
- The industry should follow the guidance set out by global and regional frameworks to which the Government of Cambodia has committed and is guided, including the INSPIRE Strategies to End Violence Against Children, and the Model National Response to prevent and respond to online child sexual exploitation. These frameworks require that the industry work closely with other sectors of society, including the child protection and welfare system, education, health, justice and law enforcement.
- At the regional level, the ASEAN Regional Plan of Action for the Protection of all Children from Online Exploitation and Abuse, clearly details the role of the digital technology industry, as does the ITU/ASEAN Child Online Protection Framework. Nationally, the Action Plan to Prevent and Respond to Online Child Sexual Exploitation and Abuse, and the Cambodia Child Protection Strategic Implementation Plan 2022-2026 (under development), have reference. The draft Law on Child Protection, Law on the Suppression of Human Trafficking and Sexual Exploitation, and the draft Cyber Crime Law, along with the Cambodian Penal Code, provide the key national legislative instruments.

The UN Guiding Principles on Business and Human Rights

Businesses of any sort have clearly defined responsibilities to ensure that the fundamental rights of all people including children are respected and promoted in all aspects of what they do. The actions of businesses can affect individual's enjoyment and realisation of their human rights, either positively or negatively. The important role of business in respecting human rights are set out in the United Nations Guiding Principles on Business and Human Rights (UNGPs). These principles set out the framework for respecting and protecting human rights, and providing remedies when individuals' rights are violated by businesses. The UNGPs set out that the International Bill on Human Rights and the International labour Organization's (ILO) core conventions[10] should provide the reference point for businesses of any kind to understand human rights, asses their own practices in relation to rights and how their own actions and activities might affect them, and how to mitigate the risks that any actions of the business might present.

The UNGPs is premised on three pillars:

1. The State's duty to protect against human rights abuses by third parties including businesses through regulations, legislation and policies
2. The corporate responsibility to respect human rights by avoiding infringement of others' human rights and addressing negative human rights impacts they have made through their business operations
3. The State's duty to take appropriate steps to ensure that those affected have access to effective remedies and to facilitate State- and non-State-based grievance mechanisms when rights have been violated or abused by businesses.

There is increasing focus on laws and regulations to ensure that the digital technology industry globally is acting proactively and is held accountable by States for respecting human rights, and in particular children's rights. This extends to ensuring responsibility and remedies for poorly designed products and services that maximise revenue over the safety and wellbeing rights of users; for tighter, minimized and more transparent use of user's data, and to imposing fines, penalties and other legal remedies for breaches of rights and for non-compliance. States, including Cambodia are moving to make businesses accountable for respecting child rights. Businesses thus need to think not only in terms of revenue and profit, but also in terms of how to ensure their business is sustainable within national regulatory and legislative environments. In Cambodia, this move to holding businesses accountable is evidenced in part through the Law on the Suppression of Human Trafficking and Sexual Exploitation (2008), as well as the forthcoming Cyber Crime law, and the roles and responsibilities placed on the national Regulator.

The second pillar, that of the corporate responsibility to respect human rights including vulnerable population like children, establishes a global standard for expected conduct amongst

[10] These include at minimum:
The Universal Declaration of Human Rights
International Covenant on Civil and political Rights
International Covenant on Economic, Social and Cultural Rights
Declaration of Fundamental Principles and Rights at Work

businesses. This includes, at minimum:

1. a policy statement of their commitment to respect human rights;
2. a due diligence process to assess their actual and potential impact on human rights, integrate findings and take actions to mitigate potential impact, monitor their performance and to be transparent and open about their impact; and
3. to provide remedies to those whose rights have been negatively impacted by their operations, products or services.

These commitments, and the application of the principles, apply not only to individual companies, but to those that it engages with in the value chain, to ensure that they adopt the same commitment to protecting the rights of children (see point 3, in text box below).

Lastly, the third pillar highlights the State's duty to ensure that the people affected by the negative impact from business operations have access to effective remedy. While States play primary roles in facilitating these venues, the UNGPs call for business' actions in establishing or participating in operational-level grievance mechanism for those impacted adversely by business enterprises.

Importantly, the UNGPs note that the Principles apply equally to businesses of all sizes, regardless of their sector, operational context or ownership structure. However, the Principles equally recognize that that the scale and complexity of the mechanisms and systems that businesses put in place may reflect and be proportionate to the size of the concern, while not diluting the integrity of the response and imperative to act.

In sum, the UNGPs place critical 'responsibility' on business as a member of society at large to operate their business in a way that does not violence any human rights, including those of vulnerable populations like children, and to actively contribute to the operational-level grievance mechanisms to efficiently and appropriately address human rights harms done by business.

The UNGPs, and the processes detailed therein, provide the wider framing for a more specific focus on children's rights, and how industry, and in this case the digital technology industry, can directly impact positively, and negatively, on the collective rights of children, including the right to protection.

BOX: Key features of corporate responsibility to respect human rights

1. The responsibility relates explicitly to the risks to human rights that can result from companies activities and business relationships
2. Identifying and addressing human rights risks effectively requires an understanding of those who might be affected; and of those who might be affected; and
3. the responsibility to respect human rights extends across all areas of the companies own activities, and those of it's business suppliers.

(Source: UN Guiding Principles on Business and Human Rights)

Children as rights holders warranting special protections

While human rights, and the governing Conventions and protections, apply equally to children and adults, children everywhere have certain rights that recognise the vulnerability and situations that children face by virtue of their developing age and capacities. These special considerations are protected by international conventions. The most important of these is the Convention on the Rights of the Child, which sets out 32 rights to which all children are entitled and which are guaranteed to them. These rights apply to all children, and all state parties who have ratified the convention, including Cambodia, and are expected to ensure that proactive steps are taken to protect these rights.

The safety and wellbeing of children online cannot be separated from the broader rights that children have. Underpinning the safety of children is the rights that all children have, enshrined in the Convention on the Rights of the Child, to protection from all forms of harm (Article 19), and from all forms of sexual exploitation and sexual abuse, from abduction sale or trafficking, and any other form of exploitation (Art. 34-35).[11] It is thus impossible to talk about the protection of children from Online Child Sexual exploitation (OCSEA) and all forms of technology-facilitated violence, without talking about the rights of children.

The growing importance of the internet and technology in children's lives, and the opportunities that they present, demand that while ensuring children are protected online, the full range of opportunities that the digital world presents to children are not curtailed. For example, the right to be safe online should not come at the cost of the rights to education, information, or healthcare, for example, all of which children can increasingly access online, and are reliant on. Equally, research from around the world has shown that when children are not safe online, they are not able to fully realise the benefits that exist for them through the internet and technology.

Children's Rights and Business Principles

The Children's Rights and Business Principles (CRBP) developed by UNICEF, the UN Global Compact, and Save the Children, build on the foundation laid by the UNGPs, and detail how businesses can respect and support the rights of children specifically in the workplace, the marketplace, the community and the environment as warranting special consideration. The CRBP recognize that children may often be disproportionately violated their rights by businesses and may need additional considerations and measures that reflect their specific stages of development, ages, and capacities. The CRBP identify ten principles for business to adhere to, to ensure children's rights are respected.

Businesses should:

1. Meet their responsibilities to respect children's rights and commit to supporting the human rights of children.

In the workplace,

2. Contribute to the elimination of child labour in all business activities and business practices.
3. Provide decent work for young workers, parents and caregivers.

[11] United Nations Committee on the Rights of the Child. (1989). Convention on the Rights of the Child. General Assembly Resolution 44/25, 20 November 1989.

4. Ensure the protection and safety of all children in all business activities and facilities.

In the marketplace,

5. Ensure that products and services are safe and seek to support children's rights through them.
6. Use marketing and advertising that respects and support children's rights.

In the community and the environment,

7. Respect and support children's rights in relation to the environment and land acquisition and use.
8. Respect and support children's rights in security arrangements.
9. Help protect children affected by emergencies.
10. Reinforce community and government efforts to support and protect children's rights.

Figure 1. United Nations Child Rights and Business Principles[12]

When it comes to the child online protection challenges, business often requires reassessment of the fifth pillar '5. safe products and services for children,' speaking with the CRBP term. The fifth principle urges business to respect children's rights by ensuring that the research, design, and testing of products and services potentially being used by children meet the national and international standards, ensuring that the products and services do not cause mental, moral or physical harm to children, restricting access to the products and services that may cause them harm while respecting freedom of expression and access to information, and preventing the risks that the products and services might entail in abusing, exploiting and harming children in any form.[13] By specifying existing and potential risks unique to children, the CRBP articulates the expected actions for the business world to respect and support children's rights.

[12] Children's Rights and Business Principles (CRBP)

[13] Children's Rights and Business Principles – pillar 5 (p.24)

Underpinning every facet of both the UNGP and the CRBP, and their application to and by business, is the notion of and commitment to the principle of Do No Harm.

Protecting children's rights in the digital environment

Until recently, a lack of evidence on what works to keep children safe online had led to approaches to online safety that restrict children and young people's access to technology and the internet. Now, a growing body of research and evidence is allowing us to better understand how to protect children's opportunities and rights online, while keeping them safe.[14] The digital technology industry has a central role to play in working actively to ensure these rights are achieved and protected.

In January 2021, the CRC took a landmark decision in its adoption of the General Comment 25 (GC.25), noting that all children's rights apply equally online as offline, and that there should be no distinction between the digital and offline environment.[15] Importantly, the General Comment also provides guidance on the realization of children's rights in the digital environment. As such, the need to balance the right to safety and protection online with the opportunities that are presented, are enshrined in the interpretation of the Convention on the Rights of the Child. The GC.25 also provides four cross-cutting principles which are central to achieving children's rights in the digital environment: non-discrimination, best-interest of the child, the right to life, survival and development; and respect for the views of the child.

GC.25 requires states (amongst others) to take measures, including through the development, monitoring, implementation and evaluation of legislation, regulations and policies, to ensure compliance by businesses with their obligations to prevent their networks or online services from being used in ways that cause or contribute to violations or abuses of children's rights, including their rights to privacy and protection, and to provide children, parents and caregivers with prompt and effective remedies.

These principles have direct bearing on all aspects of the products and services that the digital technology industry in Cambodia offer, and on the responsibility of the Royal Government of Cambodia to ensure that the digital technology industry:

- take into account how all products and services benefit all children, including those with disability; those who may not be able to afford the services and so are meaningfully disadvantaged from the realisation of other rights, such as education; or those who may live in rural areas;
- always consider whether the products and services, particularly those targeting children, are likely to be in the best interest of the child, or whether they may pose risks and undermine the best interest of the child;

[14] See for example, Stoilova, Mariya; Livingstone, Sonia; Khazbak, Rana (2021). Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes, Innocenti Discussion Papers, no. 2020-03, UNICEF Office of Research - Innocenti, Florence

[15] United Nations Committee on the Rights of the Child. (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment. CEC/C/GC/25. 2 March 2021.

- always assess whether the products or services that they deliver undermine or threaten the life, survival or wellbeing of the child, or may impact on their development in any substantive ways (this includes products that may introduce risks into children's lives that may impact negatively on cognitive, health or educational development outcomes);[16]and
- always consider what children themselves think, experience, and voice, about their experiences of products and services, as they are best suited to reflect their own experiences, rather than having those experiences and views imposed on them by adults.

The GC.25 speaks directly to the role of the private sector in protecting children's rights in the digital environment: the GC.25 calls on member States – all those who have signed and ratified the Convention on the Rights of the Child - to ensure that the private sector undertake due diligence on the impact of their products and services on child rights in the digital space (Art. 38), and to take steps to monitor, prevent and act against businesses who infringe on the rights of children as enshrined in the Convention (Art. 39).[17]

Even more specifically, the GC.25 notes the imperative on businesses to respect their "obligations to prevent their networks or online services from being used in ways that cause or contribute to violations or abuses of children's rights, including their rights to privacy and protection, and to provide children, parents and caregivers with prompt and effective remedies" (Art. 36).

BOX: Online Violence, or Technology-Facilitated Violence?

Online violence is increasingly referred to as technology-facilitated violence. This is not by accident but is an important step in recognizing the complex nature of violence that occurs and is experienced by children when using digital technology, or when 'online'. As digital technology is increasingly seamlessly integrated into children's lives, the online-offline distinction becomes increasingly artificial.

The violence that children experience when using technology is also, increasingly, embedded within broader life experiences in the offline space. Violence, such as bullying, may start online (cyberbullying) and then move into the physical space (bullying), or sexual exploitation and abuse may start offline and then move online, or vice-versa. Like many aspects of children's lives, the distinction between online and offline in relation to violence is becoming artificial. For this reason, the use of technology-facilitated violence, where technology is used in the act or experience of violence is a better reflection of the lived reality.

This also means that the digital technology industry, in its role in preventing and responding to technology-facilitated, can and should make a very real impact on violence that may occur in the offline space as well.

[16]A useful operationalization of risks, as content, conduct, contract and contact risks, can be found here: Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz- Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

[17] United Nations Committee on the Rights of the Child, 2021

This explicitly places a responsibility on all businesses within the digital technology industry to ensure that their products are safe for children to use, while also protecting all the concurrent rights of the child – most significantly in this context the right to protection from harm, to information, to participation and to education – in and through the products and services that they develop and deliver. Further, it places the onus on the State to ensure this happens, and to take actions when businesses violate the rights of children. As such, the provisions within the GC25 provide a specific application of the UNGP and CRBP to the digital technology industry, and provides a lens through which the ICT and digital technology industry in Cambodia should adopt a balanced and child rights-centered approach to keeping children safe online.

These Guidelines are an important step towards the Government of Cambodia's obligations, along with the regulation of the digital technology industry in Cambodia, in that regard.

Technology facilitated violence and online child sexual exploitation

Online violence, or technology facilitated violence, encompasses a wide range of violence against children. Understanding the different forms of violence, such as cyberbullying, image-based sexual abuse or doxing, for example, experienced by children when online, or through the use of technology, is important if steps are to be taken to create safe online environments for all children.

Online child sexual exploitation can take many forms. Along with cyberbullying, OCSEA is the form of violence that is most commonly prioritised by governments, policy-makers, industry and practitioners. Although it is constantly evolving, OCSEA generally includes:

- the grooming or online solicitation of children for sexual purposes (grooming can start offline and move into the online space, or can be initiated through the use of technology, such as social media and messaging sites, or even gaming platforms, and move into the physical space),
- child sexual abuse material (CSAM), also known as child pornography,
- livestreaming of sexual content,
- image-based sexual abuse (including the non-consensual sharing or creation of images, and image-based sexual harassment),
- sexual harassment or stalking.

While some forms of OCSEA are currently defined in law in Cambodia, not all forms of internationally recognized OCSEA are contained within the current Cambodian legislative framework and criminal code. Several key legal texts are currently being revised and will better align with international norms, including the draft Law on Child Protection. However, this does not mean that the Cambodian technology industry should not act to prevent OCSEA in all its forms as contained and referenced in international instruments, including those to which the Government of Cambodia is party. A collective agreement to this will create both a level playing field for companies of all size to act against OCSEA, and will further the effectiveness of the response of companies within the broader global landscape.

BOX: A Common Definition of OCSEA For Cambodia

Online Child Sexual Exploitation is "Any use of information and communication technologies (ICTs) that results in or facilitates sexual exploitation or abuse or causes a child to be sexually exploited or abused or that results in or causes images or other material documenting such sexual exploitation or abuse, both real or simulated, to be produced, bought, sold, possessed, distributed, or transmitted. OCSEA includes grooming, indecent images or videos of children taken through coercion, threats, force, deception or persuasion or through peer-to-peer sharing, and use of children in audio or visual images of child abuse." (Adapted from RPA)

Although the terms are sometimes used interchangeably, what distinguishes the concept of child sexual exploitation from child sexual abuse is the underlying notion of exchange, financial or otherwise.

It is important that the digital technology industry in Cambodia agree and act on a common understanding of Online Child Sexual Exploitation and Abuse. This will ensure that consistent decisions and actions are taken on all forms of OCSEA equally, but all digital technology companies within Cambodia, acting equally and fairly. This definition should be consistent with international definitions as far as possible, as acting to deal with many forms of OCSEA require the cooperation of international agencies (such as INTERPOL), and at times, other countries, as well as global technology companies who recognize and commit to acting on these common definitions.

Importantly, OCSEA can be committed by anyone, whether they be strangers or people known to the victim. The idea of "stranger danger" often drives efforts to prevent and respond to OCSEA, thus neglecting the risks and potential harms that can be posed by people known to the victim. These sexual risks may come from people within the child's immediate or extended family, online or offline community, school or friends. For example, recent evidence from Cambodia shows that in the most recent experience of different forms of online grooming – requesting sexual images or content, or being asked to talk about sexual things – as well as sexual exploitation, the requests most commonly came from family members of the child.[18]

Cyberbullying refers to what is usually (but not always) an intentional pattern of hurtful behaviour which typically involves elements of power imbalance, inflicted through the use of digital technology. Cyberbullying may overlap with offline bullying (relational context and school), and often starts offline and moves online, or conversely, may start online and move into the offline space. Cyberbullying, like any other form of bullying, can escalate to serious harms to children, in the most extreme of cases resulting in self-harm or the loss of the victim's life.

[18]Kardefelt Winther, Daniel (2022). Disrupting Harm in Cambodia: Evidence on online child sexual exploitation and abuse, Innocenti Research Report, UNICEF Office of Research - Innocenti, Florence.

With all these forms of technology-facilitated violence, it is important to remember that one form of violence is often linked to other forms of violence. Evidence increasingly shows that children who are at particular risk to experience technology-facilitated violence are also at increased risk of experiencing offline violence.[19] Similarly, children who experience one form of technology-facilitated violence, such as image-based sexual abuse, may be at increased risk of experiencing cyberbullying. It is also important to remember that one cannot view one form of violence as more severe or important than another, as different forms of violence do intersect, and may impact on different children in different ways.

Certain groups of children may also be at disproportionate risk of experiencing technology-facilitated violence. Children with disabilities, for whom technology is arguably even more important, tend to be at greater risk of experiencing technology-related violence than other children. Children who live on the street, displaced children, and other minorities, have also been shown to be at greater risk of experiencing violence.[20] Levels of digital literacy, also correlated with the ability to successfully navigate risk, may also be lower within these groups of children, thus disproportionately placing them at even greater risk of experiencing technology-facilitated violence. This means that the digital technology industry needs to take into account the needs of all these children in thinking about its role in preventing and responding to technology-facilitated violence, and in protecting children online.

Children's experiences may also be shaped by the specific platforms that they use. While social media and chat platforms are the most common apps used by children in Cambodia, the specific application types may present particular experiences of risk, and of potential harms. Some examples of how these experiences may be shaped by different platforms are presented in the table below.

Different forms of online sexual exploitation and abuse provide slightly different examples. Often, the initial contact between a potential sexual predator with a child takes place online, through social media, multi-user games or other online platforms. This contact can develop, under the guide of an online relationship, before escalating to an actual physical meeting, moving the incident from a purely online space to what is more usually considered offline grooming and sexual exploitation. This abuse can then take place purely offline, or can retain an online component if the contact continues both online and offline.

Table 2. Examples of feature-specific-technology facilitated violence[21]

Social media (user-generated and content hosting)	Context: social media is central to children's lives and how they communicate. It can offer the opportunity to develop key skills, to explore their identity in safe environments, and learn more about the world.

[19]World Health Organization. What works to prevent online violence against children? Geneva: World Health Organization; 2022. Licence: CC BY-NC-SA 3.0 IGO. https://creativecommons.org/licenses/by-nc-sa/3.0/igo/

[20]UNICEF East Asia and the Pacific Regional Office and the Centre for Justice and Crime Prevention (2020). Our Lives Online: Use of social media by children and adolescents in East Asia - opportunities, risks and harms. UNICEF, Bangkok https://www.unicef.org/eap/sites/unicef.org.eap/files/2020-02/Our%20Lives%20Online%20-%20Children%27s%20use%20of%20social%20media%20in%20East%20Asia.pdf

[21]Adapted from ITU (2022). Guidelines for Industry on Child Online Protection

	➥ Children's view of privacy on social media is often constructed in relation to friends and peers, rather than strangers and third parties. This can leave them vulnerable to commercial contract data exploitation, grooming, or commercial sexual exploitation ➥ These privacy concerns extend to the sharing of explicit images without consent. While the GC.25 makes clear that the consensual production and sharing of self-generated images should not be criminalized, the non-consensual sharing of such content may pose a great risk to children, and may even open them up to prosecution, above the risk of shaming, bullying, negative mental health consequences and other potentially harmful outcomes.
Online gaming	Context: Gaming has become increasingly important for many children, and for many through the COVID pandemic and beyond, the only opportunity for play. In Cambodia, online gaming has become increasingly accessible through mobile games. ➥ While gaming has been shown to be beneficial to children's development in many ways, such as the development of fine motor coordination and problem solving and may provide an importance sense of community and belonging for children, games can pose significant risks to children if left to play without support, and for younger children, supervision. In-game apps and functionality such as chatting and image sharing can pose similar risks to those presented by the abuse of social media, including exposure to hate speech, cyberbullying and age-inappropriate content, as well as the potential for grooming. Certain in-game features can also be used to monetize cand exploit children financially through loot boxes and in-game purchases, as well as commercially and otherwise exploit children's data.
Internet of Things	Context: As the Internet of Things (IOT) gains traction both within Cambodia and globally, children's experience with digital technology may be further shaped through the inter-operability and expanded data collection and harvesting mechanisms that sit behind these systems. This extends from SMART TV's, internet-enabled SMART household features (such as security cameras, doorbells, or digital assistants), to baby monitors. ➥ These may pose risks to children's data privacy and may also expose children to unwanted contact (particularly sexual), and other risks.

Understanding Risk

The assessment and mitigation of risks to children, and the impact of risks on individuals and children's rights as enshrined in the Universal Declaration of Human Rights and the CRC are central to the UNGP and CRBP. These both explicitly note the obligation on companies to anticipate and mitigate risks that children may encounter in the use of their products or services.

It is important that companies within the digital technology industry have a common understanding of risks, so that all operate from a common understanding of what may impact negatively on the safety and wellbeing of children, and to avoid children using their products coming to any harm as a result of that use. It is also important that a common understanding exists that not all risks result in harms to children, and that some, age-appropriate risks, are important for children to learn how to navigate risks online. This capacity is age-dependent, and dependent on the levels of digital skills and education of each child.

Despite some definitional issues, there has been general consensus that risks can be categorized into four categories or typologies: content, contact, conduct, and more recently, contract. Content risks include exposure to any unwelcome or inappropriate media or content; contact risks describe any incidences where the child participates in risky communication, and conduct risks refer to scenarios where the child themselves behaves in a way that contributes to risky content or contact.

> Age can be an important risk factor in both online and offline sexual abuse. Developmental risks change for children online, depending on their access to technology, time spent online and activities they engage in online, as well as other important social and cultural factors that may shape their development.

Online risks can include a number of different experiences, from privacy invasions, and bullying, to encountering racist, hateful, violent or pornographic content, each of which can be categorized according to the typology presented above. An example is reflected in the table below (see Figure 2).

With the massive growth of the commercial use and potential exploitation of children's data (and children) for commercial gain by industry and the private sector, a fourth risk category has recently been added to the above typology, that of contract risks. These are illustrated in the diagram below. Thinking about risks in this way allows for different sectors within the digital technology industry to put in place specific measures to address each. Some risks will be more relevant to specific services and products, while other risks will be more relevant to others within the digital technology industry.

Figure 2: Typology of ICT-related harms

CO RE	Content Child engages with or is exposed to potentially harmful content	Contact Child experiences or is targeted by potentially harmful *adult* contact	Conduct Child witnesses, participates in or is a victim of potentially harmful *peer* conduct	Contract Child is party to or exploited by potentially harmful contract
Aggressive	Violent, gory, graphic, racist, hateful or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
Sexual	Pornography (harmful or illegal), sexualization of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
Values	Mis/disinformation, age-inappropriate marketing or user-generated content	Ideological persuasion or manipulation, radicalisation and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
Cross-cutting	**Privacy violations** (interpersonal, institutional, commercial) **Physical and mental health risks** (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) **Inequalities and discrimination** (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

Source: Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

APPLYING GLOBAL AND REGIONAL COP FRAMEWORKS TO THE DIGITAL TECHNOLOGY INDUSTRY IN CAMBODIA.

SECTION SNAPSHOT:

- The digital technology industry in Cambodia should be guided in its response to OCSEA and its child rights obligations by the various global and regional frameworks that exist, all of which reflect the CRBP. These include the Model National Response to End Online Child Sexual Exploitation and Abuse, the INSPIRE Strategies to End Violence Against Children, and the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN. The industry should also adhere to the Child Online Protection Guidelines developed by the International Telecommunications Union (ITU), which provide further guidance specifically for industry. These are all framed within the UNGP on Business and Human Rights.
- The MNR explicitly requires the digital technology industry to take steps to act on notice and takedown orders, to report OCSEA, to act on solutions to prevent OCSEA, and to engage in child-focused corporate social responsibility activities.
- The INSPIRE strategies have as core strategy the creation of safe environments – and these should include the digital environment – and education and lifeskills programme, which should constitute one aspect of the digital technology industries CSR response.
- The ASEAN RPA has 7 focus areas, of which the seventh is dedicated to the role of industry in preventing OCSEA (and indeed all forms of online exploitation and abuse). Reflecting the MNR, this includes the establishment and implementation of notices and takedown orders, establishing effective reporting mechanisms, amongst others.
- Note that Cambodia is obligated at a national level to develop national responses in line with the MNR, through its membership of the WeProtect Global Alliance, and as a Pathfinding country, to implement the INSPIRE strategies.
- Two other national-level documents also have direct relevance to the role of Industry in Cambodia in keeping children safe online. The 2023 CNCC National Guidelines on Online Child Protection explicitly notes the role of the digital technology industry in COP, while Chapter Six of the Draft Law on Child Protection (February 2023 draft) details the location of COP within the broader Child Protection system, and application of the pending legislation to this form of child protection. Both of these have been informed and are aligned with the ASEAN RPA and the MNR.

The digital technology industry, digital technology and the internet are by very nature global, connected to and dependent on relationships, contacts and environments spanning across countries, regions and the globe. Given this, any attempt to develop strategies or policies to keep children safe online, need to be located within global contexts, and consider the merging of both hyper-local risks and potential harms, and the international nature of many forms of risks that children encounter online, and potential harms that may result from being online.

Several frameworks, strategies and guidance exist at a global level to assist countries to develop prevention and response strategies to address all forms of online violence against children, as well as more focused guidance on online child sexual exploitation. These range from country-level strategies such as the Model National Response (MNR), developed by WeProtect to address OCSEA and the Seven INSPIRE Strategies to End Violence Against Children (INSPIRE).

Related to this is the Regional Plan of Action (RPA) for the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN (2020), a supplemental plan to the ASEAN Regional Plan of Action on the Elimination of Violence Against Children.

In addition to these are industry and stakeholder-specific guidance, that offer specific protocols and assistance to identified stakeholders, within which more detailed actions, directly relevant to their operating context, can be formulated by each of these different stakeholders to prevent and respond to OCSEA and all forms of online violence against children. Examples of these include the ITU Guidelines for industry, for parents and schools, and for policy makers on Child Online Protection.

The Model National Response

The Model National Response is a model framework developed by countries within the WeProtect Global Alliance, for countries to adopt, and against which they can assess themselves, to address OCSEA. This is important, as Cambodia is a partner of WeProtect and is approaching its country level response to addressing OCSEA within the framework of the MNR. The MNR explicitly informed the development of the forthcoming CNCC OCSEA Action Plan. While not based on specific bodies of evidence, it offers different thematic areas or "capabilities" in which specific national and local level activities can be tailored to deliver targeted positive outcomes for children. These include:

1. Policy and legislation
2. Criminal justice
3. Victim
4. Societal
5. **Industry**
6. Media and communications

The MNR cuts across domains and sectors of society, but has a specific capability focusing on Industry, and its role in preventing and responding to OCSEA. Specifically, the industry capability requires that the digital technology industry in a country:

- Acts on notice and takedown procedures,
- Is directed by statutory protections that allow industry to fully and effectively report OCSEA, including its transmission, to the designated (law enforcement) agency,
- Engages in innovative solutions development to help address local OCSEA issues, and
- Engages in effective child -focused corporate social responsibility.

An important dimension of the MNR is its emphasis on effective leadership and coordination of the different individual response areas involved in addressing ICT-related violence and abuse. Where previously interventions to tackle ICT-related violence and abuse focused on response and support systems, for instance through helplines and hotlines for reporting abuse and targeted victim support, the MNR adopts a wider societal perspective, across which the digital technology industry must play an important role if it is to adhere in full to its collective obligations under the UNGP and CRBP to protect and ensure the rights of children, discussed earlier.

The INSPIRE Strategies: Seven Strategies to End Violence Against Children.[23]

The INSPIRE strategies are seven evidence-base strategies to end violence against children, developed by the World Health Organization, UNICEF and other international agencies. These strategies focus on seven areas:

1. Implementation and enforcement of laws,
2. Norms and values,
3. **Safe environments,**
4. Parents and caregiver support,
5. Income and economic strengthening,
6. Response and support services, and
7. **Education and lifeskills.**

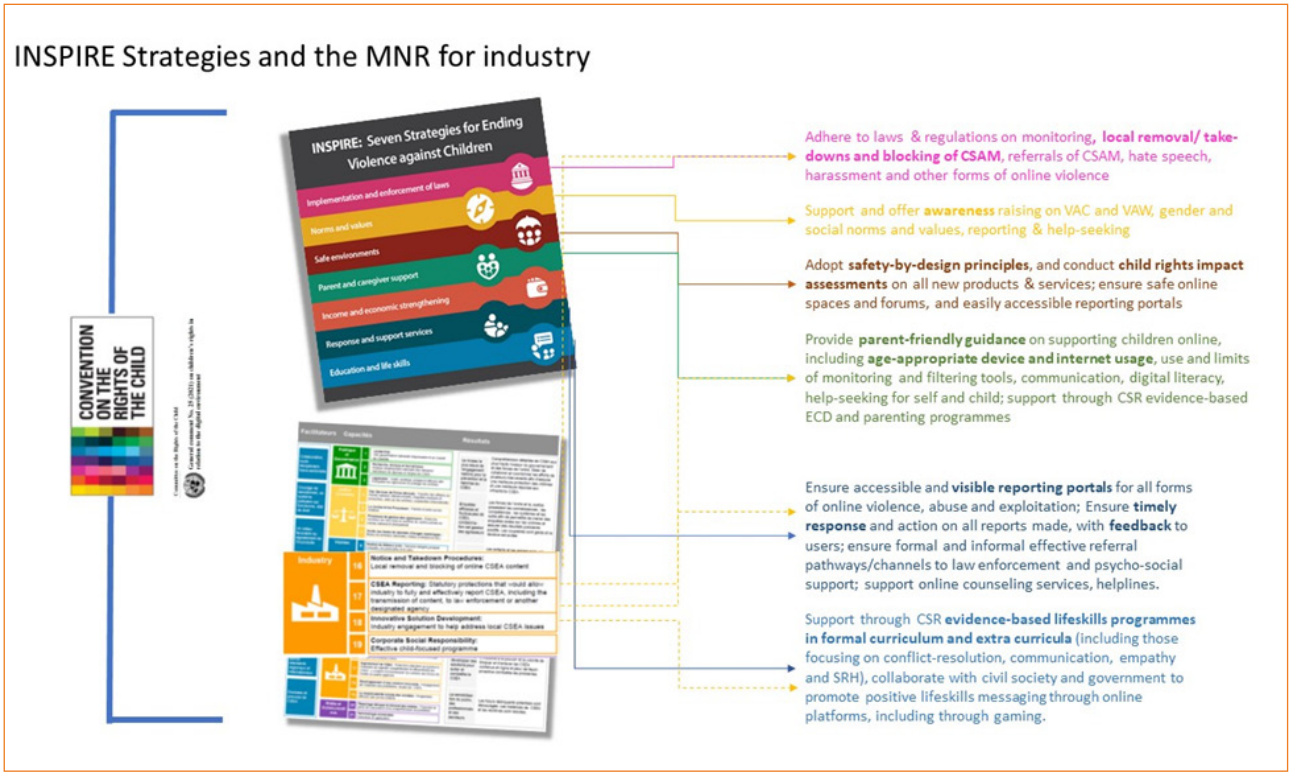
While the digital technology industry has roles to play in each of the seven INSPIRE strategies, strategy Three – Safe Environments – can translate directly to responsibilities of the industry. In INSPIRE, this refers to the importance of providing safe physical environments for children. The technology industry has a critical role to play in providing and promoting safe digital environments for children – digital platforms, applications, and services that take into account the needs and rights of children from the outset, from the very conceptualization and design of the service or product. This consideration of the potential impact on children can be institutionalized through the adoption of tools such as Child Right Impact Assessments and Safety-By-Design and Privacy-By-Design Assessment tools.[24]

The digital technology industry often supports and engages in various programmes that fall directly within the INSPIRE strategies, such as raising awareness of online risks, training and raising awareness of safety mechanisms, promoting the reporting of adverse online experiences and criminal and risky content or experiences, and supporting digital literacy and online safety programming for parents and children. This is an important role that is explicitly in line with both the MNR and INSPIRE, and also consistent with the CRBP, as one, of many, critical step in mitigating potential risks that children might face through the use of products and services.

[23] A framework for monitoring the implementation if INSPIRE, including indicators, is available here: https://cdn.who.int/media/docs/default-source/documents/child-maltreatment/inspire-indicatorguidance-resultsframework.pdf?sfvrsn=7bb60fb5_5&download=true. This could be used to inform the development and adoption of indicators to assess it's implementation through industry action.

[24] See for example, the UNICEF Mobile Operators Child Rights Impact Assessment tools; eSafety self-assessment tools ; the Tech Coalition self-assessment tool; and GSMA's Notice and Takedown process. These and other resources are provided at the end of this report.

Figure 3. How INSPIRE and the MNR align in practical actions for Industry



The Regional Plan of Action for the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN

The Regional Plan of Action (RPA) for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN (2019) is a supplemental plan to the ASEAN Regional Plan of Action on the Elimination of Violence Against Children. The RPA sets out to strengthen collective efforts across sectors and borders to effectively prevent and respond to all forms of online violence and exploitation., and to enhance international and regional cooperation with external parties, including international law enforcement agencies, civil society, UN agencies, community and faith-based organizations, academia and the private sector. The RPA is aligned with both the MNR and the INSPIRE strategies, and is also aligned with the Convention on Cybercrime (2016) (also known as the Budapest Convention) and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (commonly referred to as the Lanzerote Convention).

The RPA also provides recommendations and indicators to support the ASEAN states to develop and strengthen national actions plans (NAPS) that specifically address online abuse and exploitation. The RPA sets out five principles on which it is premised:

- A rights-based approach
- A multi-sectoral approach
- Cross-border collaboration
- Meaningful child participation, and
- ensuring recognition of the nexus between online and offline risks, exploitation and abuse.

The RPA sets out 7 focus areas, under which a number of detailed activities are described:

1. Promote, develop and implement comprehensive national legal frameworks in each ASEAN Member State and work towards improving child protection standards and policies on all forms of online exploitation and abuse across ASEAN member States.
2. Build the capacity of law enforcement and the judiciary
3. Encourage the establishment of a national specialized unit with an explicit remit to lead, support and coordinate investigations.
4. Ensure effectiveness of rights-based, gender and age-responsive child protection and support services and social welfare programmes
5. Strengthen data collection and monitoring, reporting and referral mechanisms, through hotlines to report online materials suspected to be illegal, including child sexual abuse material.
6. Promote a national education programme and school curricula to raise awareness of sexual and other forms of exploitation of children to empower children, young people, parents, guardians, caregivers, practitioners and community.
7. **Mobilize and enhance engagement with the private sector and other relevant stakeholders to actively involve them in monitoring prevention and response mechanisms through regulations, corporate social responsibility, and collaboration for the development of effective measures to detect, take down and report illegal content related to child sexual abuse exploitation.**

Two other national-level documents also have direct relevance to the role of Industry in Cambodia in keeping children safe online. The 2023 CNCC National Guidelines on Online Child Protection explicitly notes the role of the digital technology industry in COP, while Chapter Six of the Draft Law on Child Protection (February 2023 draft) details the location of COP within the broader Child Protection system, and application of the pending legislation to this form of child protection. Both of these have been informed and are aligned with the ASEAN RPA and the MNR.

The following section provides different mechanisms through which the digital technology industry in Cambodia can implement the systems and obligations detailed in the above, and in particular, Focus Area 7.


#PHNOMPHEN

PRACTICAL COP MECHANISMS FOR THE CAMBODIAN INDUSTRY

SECTION SNAPSHOT:

- The Cambodian digital technology industry should adopt core product and service assessment and design principles to ensure that the rights of the child are integrated into their core businesses. These apply to all sectors within the digital technology industry.
- Child Rights Impact Assessments (CRIA) should be carried out on all product and service, that will assess the potential impact on the collective and equal rights of children within each company. The results of these CRIAs should provide the basis (and baseline) for all subsequent child protection measures.
- Businesses should all formulate and implement internal child safeguarding policies and procedures intended to protect employees and children from harm, including the careful vetting of any employees who might encounter CSAM.
- Safety by design and privacy by design principles should be adopted. These ensure that the potential impact of new services and products on the safety of children is assessed at the conceptualisation and design stage of any product or service development, and the subsequent design can factor in appropriate safety mechanisms and adaptations form the start of the process, rather than retroactively. The same applies to privacy by design, which refers to an approach that designs *in* to the process basic systems that will ensure the privacy and protection of children's data. Note this does not prevent existing products and services from being assessed and re-designed or updated to ensure both safety and privacy.
- Related to this, ensure age-appropriate design for the target audience, using the developmental and evolving capacity of children as a guide.
- Develop evidence based OCSEA and CSAM prevention and response mechanisms and institutionalise these into the company and all products, as informed by the results of the CRIA. Steps to be taken include:
    - Establishing a single contact point, usually within the operational or technical division of the company, or trust and safety units where they exit, for all reports and handling of CSAM. This position or unit should receive appropriate and ongoing training, and be carefully screened for suitability for the position, including any prior record of child-related offences. Provision of appropriate care and support, including psycho-social support, to those who are responsible within companies for dealing with CSAM, should also be provided.
    - Develop clear company-wide policies that explicitly state a zero-tolerance approach to CSAM and OCSEA, along with internal reporting and grievance mechanisms.

- Create and publicise easy-to-use, accessible reporting services in apps, platforms or websites where users and members of the public can report suspected CSAM or other forms of technology-related violence. These services should be accompanied with clear feedback and accountability mechanisms to ensure that those making reports are updated on the process, and annual transparency reports on actions taken, published.
- Ensure that options for referral to formal psycho-social support services, or counselling services always accompany any reports made, and where necessary referral for coordinated case management services. The MPTC can assist in the identification of reliable service providers.
- Ensure referral mechanisms for all illegal content to the designated law enforcement agency, the anti-Cybercrime Department.
- Establish partnerships or linkages with designated global reporting Hotlines, such as the IWF or ICMEC.
- Establish formal takedown and notice procedures, that set out clearly what the minimum conditions for such processes are, how these are to be made or responded to, and the related timeframes for each action.

- Invest in evidence-based messaging, building on recent evidence produced by the WHO and UNICEF,[25] on building the capacity and awareness of children and parents or caregivers, through schools, community groups and other entry points. These should ensure that adequate attention is paid to the risk that is posed to children online from peers, acquaintances and others known to the child, rather than focusing on 'stranger danger', on prevention education appropriate to the age of the child, and on supporting parents and carers to speak openly and be supportive of their child, rather than adopting punitive approaches. This can be done in part by supporting existing social and behavioural change (SBC) programmes currently being offered in schools and at a community level, rather than offering stand-alone education and awareness raising interventions, and so will require partnerships with a range of organizations in Cambodia working with children, particularly around gender-violence and other SBC programming.
- Throughout the process of adopting and instituting more child-rights focused approaches to child online protection, micro, small and medium sized companies can seek support from the MPTC in conducting CRIA, developing child safeguarding policies, and developing CSAM prevention and response mechanisms. Particular areas of support are highlighted in green throughout the chapter:

There are several existing mechanisms that the digital technology industry can use to prepare for and strengthen their prevention and response systems to better protect children online (some of these are explained in the following sections, and include the UNICEF MO-CRIA: Child Rights Impact self-assessment tool for mobile operators, the Australian eSafety Commissioner' Office self-assessment tools for large and medium technology industries, and safety by design principles produced by the same office, amongst others. These locate the specific steps that industry can take to keep

[25] World Health Organization. 2022. What works to prevent online violence against children?

These Guidelines recognize that the digital technology and ICT industry is made up of many different types of services and companies. These include social media platforms and other content creation and hosting services, infrastructure and connectivity providers (including mobile operators and internet service providers), content curation services, and Artificial Intelligence driven systems and services. Many of the steps detailed in these Guidelines apply universally and can be taken across all these different service and product types; in other cases, specific guidelines apply to specific services and products.

children safe within the broader context of child online protection and child safety online to ensure that children receive the best possible response and support from all agencies, departments and partners when they encounter risks online. The following tools build on the recommendations made in the Capacity Assessment report undertaken prior to the development of these Guidelines.

While these mechanisms are not currently mandatory within the regulatory and legislative framework within Cambodia, each of these steps below are increasingly being incorporated as mandatory within new legislation intended to hold digital technology companies accountable for children's safety.[26]This specifically include tools such as Child Rights Impact Assessments, safety-by-design principles, and appropriate proactive CSAM prevention and response mechanisms (depending on the specific legislation focus). Failure to undertake these measures come with significant penalties, that may be tailored to the size of the company involved.

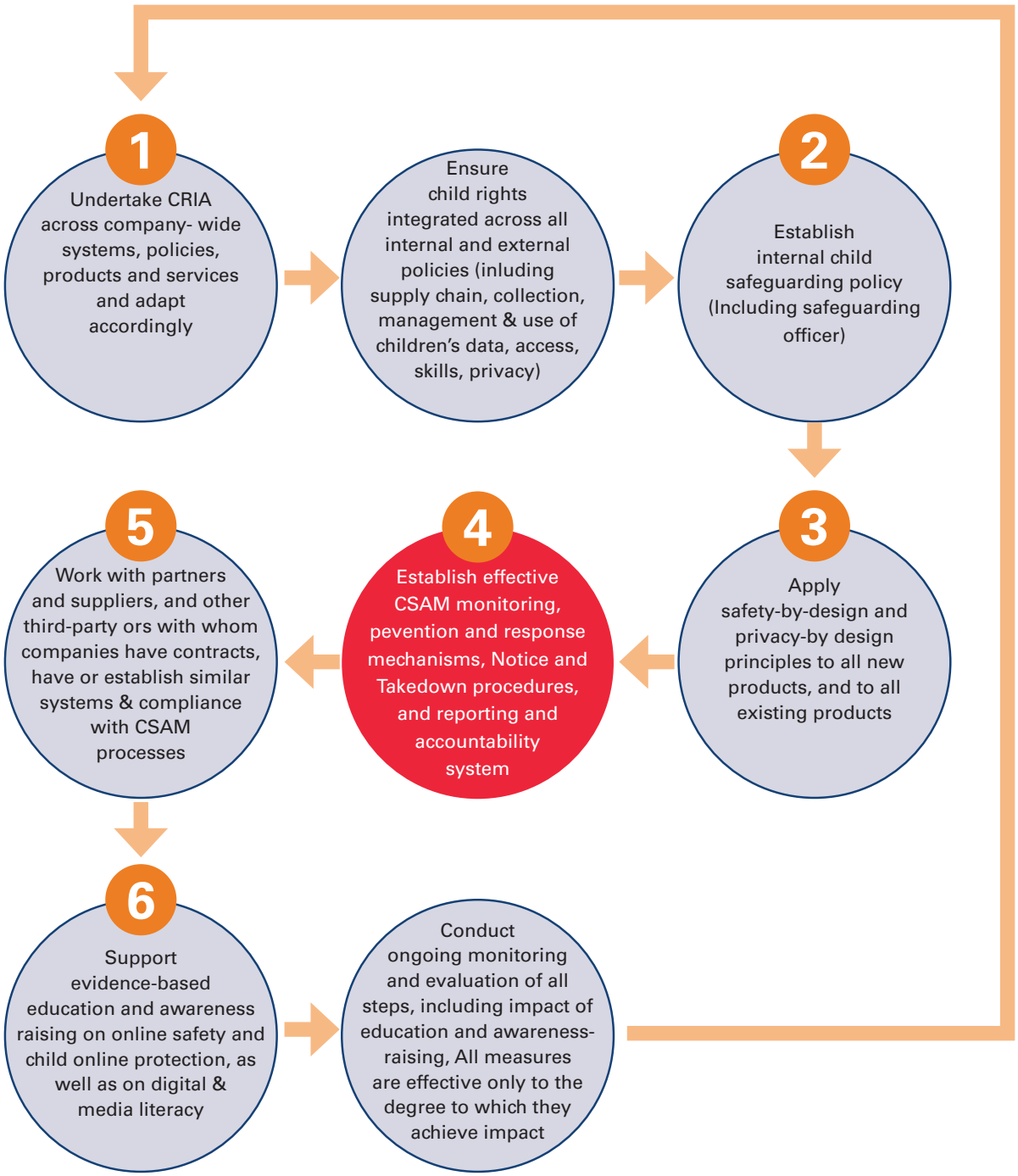
Each of these steps may also take a varying amount of time, depending on the company size, resources, and the nature of services or products delivered. More important than applying a strict timeframe for the completion of these steps, is ensuring that each is taken thoroughly, and that the results of each feed meaningfully into internal policies, strategies, and product and service design. The last step, that of monitoring, should occur in an ongoing basis (see below).

Transparency is a critical tool in accountability and can increase the public's confidence and trust in products and services. Throughout the following section, specific mention is made of the importance of publicizing, through annual transparency reports, the result of assessments and outcomes on specific metrics. These are particularly important in preventing and responding to OCSEA and CSAM. Companies should, depending on the nature of the services and products they provide, publish annual transparency reports that include, at minimum, the number of reports of CSAM and other forms of OCSEA they receive, actions taken on individual user accounts (warning, temporary suspension, permanent suspension/closure, or other actions), and reports and referrals to external authorities, and the time taken from report to action.[27]

[26]See for example, the California Age-Appropriate Design Code, 2021; the Australian Online Safety Act, 2021; the UK Online Safety Bill; the UK Age-appropriate Design Code, 2020; and the Singapore Online Safety Act, 2022.

[27]Adapted from Tech Coalition, Trust: Voluntary Framework for Industry Transparency

Figure 4. Practical steps for industry to ensure effective COP systems.



The diversity of the digital technology industry in Cambodia is recognized, with the scope of companies ranging from small and micro-enterprises and start-ups through to large national and multinational telecoms and ISP companies. While the different mechanisms described below are important for industries of any size, certain steps may be initially onerous on smaller companies with limited employees, revenue and resources. Each of these actions, processes and mechanisms can be adapted to the size and resources of the individual company.

The MPTC may also play a role in providing specialized support to smaller companies and start-ups in realising their collective child rights and child protection responsibilities

However, the size of a company should not negate the importance or institutionalisation of each, as they apply to a company of any size. A useful resource for smaller companies, including SME and tech-start-ups, including in the implementation of safety-by-design and impact assessment's, is available through the Australian eSafety Commissioner Office. It is also important that the regulation and oversight of these principles take into account the size of companies, and any penalties associated with non-compliance or proportionate to the size of the enterprise.

Adopting a child-rights centred approach to keeping children safe online: Child Rights Impact Assessments

Child Rights Impact Assessments (CRIA) are mechanisms through which industries can assess the potential impact of their products or services, from the conceptualisation and design stages through to rolling them out to market. CRIAs do not only assess impact on children's rights to safety in the digital environment but can be used to assess the potential impact on the collective rights of children online and offline (see box below). These range from the supply chain through to the products and services themselves. CRIA should serve as the departure point for due diligence to ensure that their policies, procedures and services are in line both with the Cambodian legislation and with international norms and standards. By voluntarily undertaking CRIAs companies are proactively promoting children's safety and wellbeing and advancing children's rights to access to information, freedom of expression, participation, education and culture, as detailed in general Comment No.25.[28]

UNICEF has developed a Child Rights Impact Assessment tool for mobile operators, that has been developed in partnership with several mobile operators throughout the world (UNICEF, 2021, MO-CRIA: Child Rights Impact Self-assessment Tool for Mobile Operators, UNICEF, New York). This tool provides a practical tool with which mobile operators can evaluate themselves, across the operation, to ensure that each of the 10 principles detailed earlier are adequately met, within the context of services and products that mobile operators provide. This tool consists of 5 steps:

[28] ITU, 2020, Industry Guidelines

1. Identifying colleagues to be involved in the assessment
2. Launching the CRIA self-assessment process
3. Gathering input from colleagues
4. Additional inputs to the assessment (from external stakeholders), and
5. Acting on CRIA findings

While primarily designed for mobile operators, such a tool can also be adapted and used by other providers as a departure for sector-specific assessments. It is important that at each stage of the CRIA, consideration is paid to how the company, through it's policies, processes, products and services, will impact on children who may be at significantly greater risk of having their rights infringed, such as children with disabilities, or those without care or homes. Digital technology can be even more important for many children, yet they ae often disproportionately affected by products and services that are not designed with child safety, protection and wellbeing in mind.

Throughout the CRIA, the MPTC can provide support to micro, small and medium digital technology companies to conduct CRIA and develop appropriate plans.

While there is currently no explicit requirement in Cambodian legislation for technology companies to conduct such assessments, the uniform adoption of such tools provides an important platform from which all technology companies can illustrate their commitment to ensuring the best interest of the child is considered and mainstreamed across their business practices and services. The publication of annual transparency reports on the results of their CRIA, and of all reports of OCSEA, and steps taken in response to each report, particularly for established and medium to large companies such as the mobile operators and content providers, will also provide additional incentive for companies to be proactive.

In addition to being important tools for companies to ensure that the rights of children are respected and promoted in all that they do, CRIA can also serve as important accountability tools. The results of CRIA should be disclosed in a transparent fashion to the public. This will serve both as a reflection of the integrity of the company and the priority it accords to the rights and best-interest of children and will also allow the public to make informed judgements as to the suitability of products and services.

Note that where companies have recently completed a CRIA, there is no need to undertake this step, although consideration should be given to updating the Assessment, depending on how recently the Assessment was done.

BOX: The Millicom CRIA Case Study

Telecoms provider Millicom, in partnership with UNICEF undertook a Child Rights Impact Assessment on its operations initially in the Democratic Republic of Congo, followed by Rwanda, Tanzania, Bolivia, Columbia and Costa Rica. This assessment comprised a desk review of Millicoms children's rights risk landscape, an assessment f global policies and processes through document reviews and interviews, an assessment of local policies and processes within the DRC and each of the countries, and a field study of the distribution of services with external stakeholders in each country. These assessments led to a corporate setting of priorities and a detailed action plan in each of the priority areas identified.

Internal child safeguarding policies

Digital technology companies in Cambodia should all have their own **child safeguarding and child rights policies, along with a mandatory child protection code of conduct** that apply across every facet of the company. These safeguarding policies should be formally incorporated into their bylaws or internal policies and procedures. Companies may have existing commitments, safeguards and protections incorporated into Human Resource policies that protect employees and staff from workplace harassment and gender-based harassment, or that address the use of child labour; child safeguarding requires its own dedicated policy. This should set out what the expectations are regarding the treatment of children, and the respecting of the collective rights of children, by all employees and management, and across product design and services, and what the consequences are of breaches of these expectations.

This policy becomes particularly important for those companies offering content or account hosting services and products, including ISPs and social media companies, as well as those utilising or developing AI systems. In detecting, preventing or responding to reports of CSAM, individuals employed by companies may themselves be exposed to abusive content. For example, if a platform receives a direct report of potential CSAM material on its platform, in the process of assessing or taking down the content, moderators or other staff will be exposed to the content. The potential also exists for those individuals to retain or in the worst case, themselves distribute the content, thus adding to the scale of the individual report and potential harm to the victim. A child safeguarding policy should also detail actions to be taken when any individual within that company acts to undermine the best interest and safety of any child, either directly or indirectly.

Within the child safeguarding policy, a single individual or office should be identified as responsible officer for all child safeguarding issues, complaints and oversight. This position or unit should receive appropriate and ongoing training, and be carefully screened for, or provide police record to the effect of suitability for the position, including any prior record of child-related offences.

This individual should ensure that the policy is clearly understood by all within the company and is adhered to and should be available to receive reports for any child safeguarding issues from both inside and outside the company. Note that if this individual or position is also responsible for handling of CSAM within the organization, then consideration should also be made within company policies for the provision of mental health support for the designated officer.

Adopt an Age-appropriate design code

Age-appropriate refers to the consideration of the age of the end-user of a product or service and the evolving capacities and developmental stages of a child, and associated risks, into the design and development of any new product or service. This ensures that from the outset of a product development, the impact of that product or service on children of different ages is considered. Simply, by agreeing to and adopting age-appropriate design codes, companies in Cambodia should always consider the age range of their audience, along with the different needs and developmental stages of children, in the design of their services and products. This should also take into account that even those products and services that may not be intended for children, may be used by children, and appropriate risk-based measures should be taken to minimize the potential for harm to children resulting from this use.

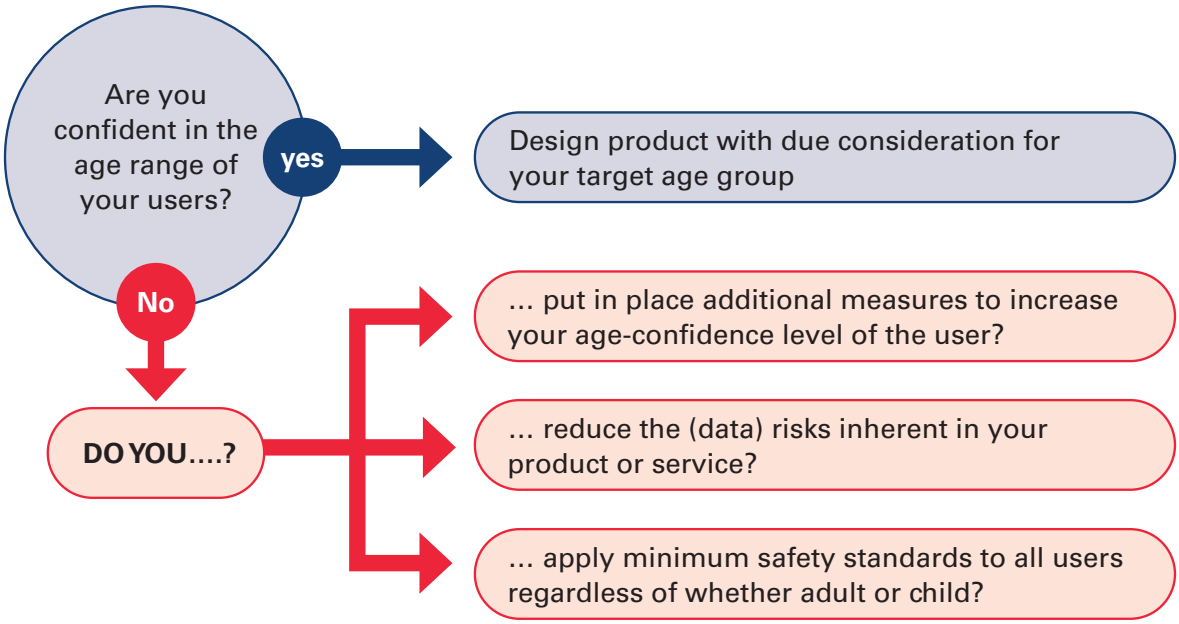
> The UK Age-Appropriate Design Code sets out 15 standards of age-appropriate design reflecting a risk-based approach. The Code requires age-appropriate default setting which ensure that children have the best possible access to services, while minimizing the data that services collect and use. It ensures that children who choose to change their default settings do so on the basis of the right information, guidance and advice provided by the service before they do so, and ensures that their data is fully protected once these settings have been changed.
>
> https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services

The UK Age-Appropriate Design Code offers useful guidelines for decision-making relating to the processing of data in an age-appropriate manner, that can be applied to the design and application of all products and services. At the heart of this is the degree of certainty that a company has as to the age of the end user of the services or products they are designing, and how it designs their products and services accordingly. This process is reflected in the figure 5 below. It provides a decision tree at the outset of the design process, that assesses the potential age of the users of the products and services, and how best to design those services and products based on a number of questions.

This process recognizes that children of different ages engage with digital technology, and content, differently, and that risks to children vary depending on the age of the child. While there is no concrete formula for determining exact parameters for what is age-appropriate in different contexts, some broad guidelines are attached Appendix 3.

One challenge faced by service providers is that it may be difficult to positively verify user's age accuracy. Any tools that may be adopted to enhance age-verification of users should be used with caution, as existing tools may result in unfair bias and discrimination, exclusion and unintentionally, infringe on other rights that children enjoy online, such as the right to participate and the right to information, if inaccurately applied.

Figure 5: Decisions in assessing the age-appropriate design of products for children[29]



Age-appropriate design also applies to the data that is collected, stored and processed in the use of products and services. Special considerations apply to the collection and processing of children's data, to ensure that their rights are protected. In the design of applications and services, technologies need to adhere to certain principles relating to children's data. General Comment No.25 states that in the collection and use of children's data, special measures are required to ensure that children's privacy is respected and protected in all environments that process their data. Four criteria are detailed. These include:

- Data minimisation: collecting the absolute minimum amount of data on children that is adequate, relevant, and limited only to the purpose to which they are processed.
- Purpose limitation: not using data collected from children for any purpose other than that for which it was explicitly collected and informing users why you need to collect use and store their data in a particular way.
- Storage limitation: storing data only for as long as is required for its stated purpose, and destroying it as soon as no longer needed for this purpose and ensuring that the data cannot be used to identify child subjects for longer than is absolutely needed for its original purpose.
- Data security: stored and processed in a way that ensures the security of the personal data including against unauthorized processing or access.[30]

The collection, processing, storage and managing of data collected from children should be a central consideration in the CRIA, age-appropriate design principles, and in the safety by design principles discussed below. The GC.25 also recommends that privacy-by-design principles, like safety-by-

[29] Adapted from the UK Age-Appropriate Design Code.

[30] Adapted from the European Union's General Data Protection Regulator (GDPR), Regulation (EU) 2016/679

design, should be integrated into digital products and services that affect children (Art. 70).There are numerous examples of the potential harms that result from contract or other risks relating to data, such as the continual foregrounding or feeding of potential harmful content such as that relating to eating disorders, being generated through ill-conceived algorithm design and minimal checks to children through social media feeds. One of the most comprehensive examples of how children's data privacy can be respected and protected can be found in the EU General Data Protection Regulations (GDPR).[31] The UNICEF's Case for Better Governance of Children's Data: A Manifesto, also provides concrete actions, priorities and commitments relating to the responsible use and management of children's data.

> Children asked the private sector for enhanced autonomy over their personal data by fully informing them of what they share, when they share, how they share, and what happens to their data.
>
> A Children's Call to Action. the ASEAN ICT Forum, November 2022

Cambodian companies and those operating within Cambodia, should thus take steps to ensure that any products or services that they design and bring to market, or offer in a third-party capacity, have taken appropriate and age-appropriate steps to protect the rights to privacy and protection that may be affected through these services. As children's lives become more 'digital by default', data collected from children is increasingly used to serve inappropriate advertising and content to children. It is also important, as per the GC.25 that wherever children's data is used, or consent is sought to process a child's data, consent is *"informed and freely given by the child, or depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to the processing of that data."*[32] It is important that children's consent is explained and sought in a way that is easily understood by children of different ages, and where consent is sought on behalf of the child from the parents, that parents who may not be digitally literate, or fully understand the implications of what is being asked, are able to understand in easy terms what data is needed, why it is needed, and how it will be used, managed and disposed of.

The MPTC can facilitate access for o micro, small and medium digital technology companies to new and emerging evidence on requirements, lessons and research on age-appropriate design, safety, by design, and related child-rights in the digital environment, as needed.

[31] European Union, GDPR, Regulation (EU 2016/679

[32] UNCRC, 2021, General Comment No.25, para 71

Lego Life: an example of safety and age-appropriate design

Lego designed a safe online space for children of different ages, through their Lego Life app. Children can create their own avatars and chose pre-approved anonymous names. The app has a full-time moderation team that ensures that there is always some supervision, or 'chaperoning', of the space, and integrates responsible online behaviour and digital citizenships through various in-built tools, such as a safety pledge for all children. The app also uses various mechanisms to encourage the development of healthy online and offline behaviour, through promoting empathy and positive communication with others. Before and during development of the app, Lego consulted with children themselves to find out what they wanted and needed – a critical part of any safety-by-design process. https://www.lego.com/en-us/life/digital-safety

Safety by design

Safety-by-design is an approach to designing services and products with the safety of the eventual users as central to the delivery of the product or service. It can be described as focusing *"on the ways technology companies can minimise online threats by anticipating, detecting and eliminating online harms before they occur."*[33]

Cambodian companies, across the spectrum of digital technology services (from ISPs to content and data hosting platforms) should adopt and commit to using safety-by-design principles in all new products and services.

While a relatively new concept – only initiated in 2018 – there are already guidelines and principles developed, in consultation with the digital technology industry on how companies can incorporate safety-by-design into their product development, delivery stages and ethos. It is important to emphasize that the development of these safety-by-design tools have been developed throughout with the support and engagement of the global digital technology industry, and thus fully reflect the realities of industry, and the pressures and imperatives that those sitting outside the private sector may not appreciate.

In including the potential safety impact on children at the very conceptualisation of any new product or design, and in taking steps throughout the design and engineering process, safety-by-design is an important mechanism to realise at least one aspect of integrating child rights into the digital technology sector.

A set of self-assessment tools has been developed by Australia's e-Safety Commissioner, and through a self-administered step-by-step process allow companies to both develop safe products, and to embed the consideration of children's safety in relation to the digital environment, into the operations and ethos of the company: https://www.esafety.gov.au/industry/safety-by-design/assessment-tools. Such an assessment is an important "fourth step" in ensuing a uniform, consistent and effective approach across the digital technology sector in Cambodia to child online protection, within a child-rights framework.

[33] https://www.esafety.gov.au/industry/safety-by-design

The tools cover structure and leadership within the company, internal policies and procedures, moderation, escalation, and operations of businesses. The tailored safety-by-design tools have been developed for start-ups and early-stage technology companies, and for mid-tier and enterprise scale companies.

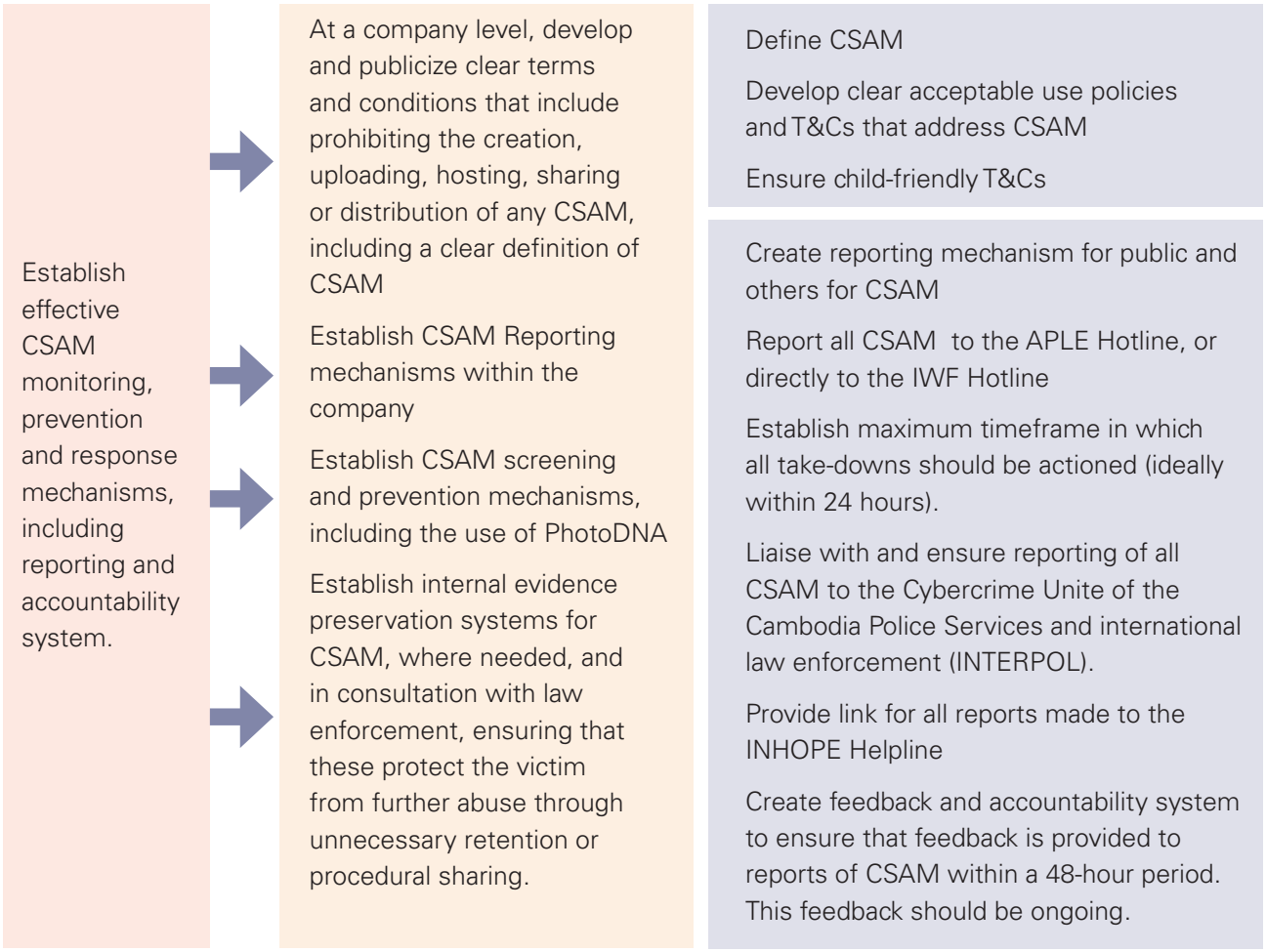
Children asked the private sector to ensure that tools and safety features, including where and how to make reports of abuse, be easily accessible and easy to use.

A Children's Call to Action. the ASEAN ICT Forum, November 2022

Preventing and responding to CSAM

The Cambodian digital technology has an important role to play in preventing and responding to CSAM. It can do this, in part, through the adoption of safety-by-design tools, but additional, dedicated processes and procedures, such as responding to Notice and Takedown procedures, are required to develop an effective CSAM prevention and response system. Each company should at minimum take the following steps to address CSAM and other forms of OCSEA.

Figure 7. A process summary for establishing CSAM systems.



1. Set out in very clear Terms and Conditions the explicit prohibition of any content or activities that may constitute CSAM, or the online sexual exploitation or abuse of children. These parameters should be clearly displayed on websites and applications. These T&Cs must be friendly to all users regardless of legal or digital expertise. For any products that are designed for children, T&Cs must be presented in a way that is easily understood by children, even if the product is not directly targeted at children but may be used by them. This should include being accessible to children with disabilities who may be using the products or services. Digital technology companies, when registering with the Ministry of Commerce and relevant authorities (including to obtain operating licenses), should make a declaration on their commitment to preventing and responding to CSAM.

2. Establish reporting portals for all content that is, or is suspected of being, CSAM, on all websites, applications or other platforms. These should be clearly visible and accessible, for both adults and children. Reports made on this platform should go directly to a dedicated CSAM desk or function within the technical division of the company, rather than to a general inquiries or customer service line function. This could be located within the same unit that deals with all cyber-security aspects relating to the company business. The reporting portal should ask the user to provide minimum information to assist with the processing and screening of the content. This should include the URL or link to the content, the nature of the material, the date and time, and provide the option of providing a contact name and contact, although this last should not be mandatory, to allow for anonymous reporting. Reporting portals should be easy accessed and understood by children and users of all ages and capacities (see box), and a set time to act and respond on each report should be established.

Proactive CSAM detection tools, including Microsoft DNA, Project Arachnid and Safer, all make use of AI systems to detect CSAM. Any proactive systems and measures to detect CSAM, OCSEA or any other form of illegal content should always be used cautiously, ensuring that the right to privacy is respected (United Nations Children's Fund (2022)). 'Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse' UNICEF, New York.

The CRC notes that any interference with children's right to privacy should be "provided by law, intended to serve a legitimate purpose, uphold the principle of data minimisation, be proportionate and designed to observe the best interests of the child, and must not conflict with the provisions, aims or objectives of the Convention [CRC]'. CRC General Comment No. 25 (2021), para. 69.

This is generally referred to as the principles of legality, necessity, and proportionality.

Reporting interfaces on websites or products may link directly to the reporting portals of authorized CSAM reporting Hotlines such as the IWF or ICMEC, if formal partnerships are in place. Another example is the STOP NCII portal, a reporting portal for non-consensual intimate image abuse (NCIIA) (also known as non-consensual sharing of self-generated images).[34] While the NCII portal is currently only for adults, a portal for child victims is currently under-development. While the burden of reporting should not be placed on the victim, it is critical that these options are available for children, and those who support children, such as teachers, when they need. Note that regardless of the size of the company, all products or services should have some reporting option for abuse.

3. Foster relationships with international agencies and partners, including those who hold or have access to CSAM image databases, such as the IWF and ICMEC, and who support CSAM Hotlines, through formal MoUs and agreements. Generally, all images are reported from various Hotlines to INTERPOL, who holds the International Child Sexual Exploitation Image Database (ICSE Database), which is used for reference by law enforcement agencies globally, including the Cambodian Police Service. In Cambodia, the MPTC will assume the position of intermediary between Cambodian companies and the ICSE database, although individual companies remain free to pursue partnerships and agreements directly with ICMEC and the IWF, as well as other partners.

For smaller companies, this could be done through a national partnership or engagement with the CSAM Hotline, which can assume the link to international agencies and partners through the INHOPE network. Support to smaller companies in developing these relationships, and in developing appropriate CSAM mechanisms, can also be provided by the MPTC.

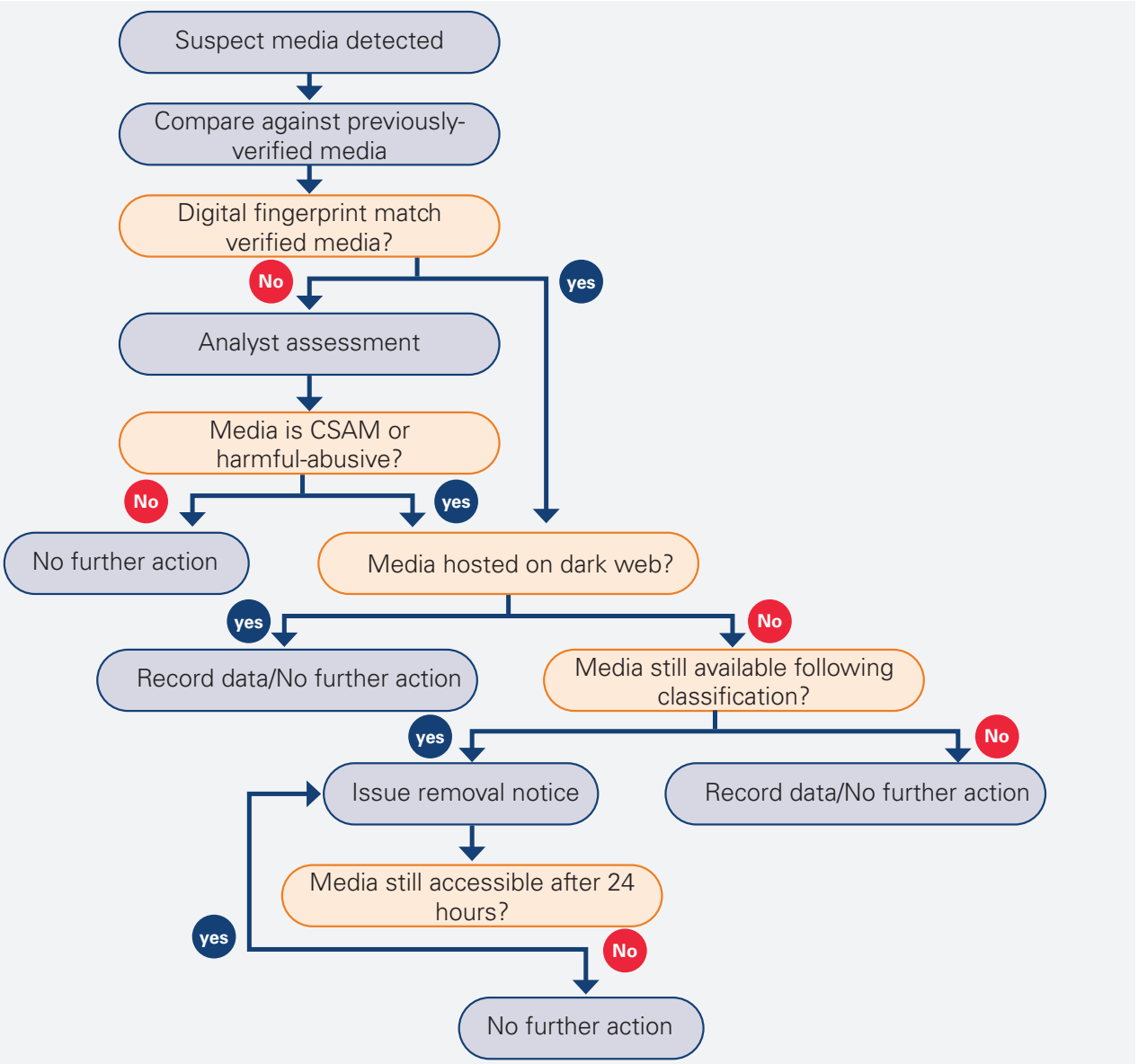
4. Consider adopting the use of free-to-use or subscription automated or AI CSAM detection tools, such as Microsoft DNA, Project Arachnid or Thorn's Safer. An example of the process utilised through Project Arachnid's API is reflected in figure 8 below. However, the use of any automated tools should ensure that they are used in a way that does not undermine children's rights to privacy in any way,[35] and is consistent with the provisions, aims and objectives of the CRC, and respects the right to privacy of children (see text box on previous page).[36]

[34] However, as of 2022 this portal is only available to adults to reports cases of NCIIA involving adults, and reports made by adults, although a similar portal for children is under development.

[35] UNICEF. 2022. Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse' UNICEF, New York.

[36] CRC General Comment No. 25 (2021), para. 69.

Figure 8: An example of a CSAM API – Thorn's Project Arachnid: how it works.[37]



Microsoft PhotoDNA is a tool that creates unique hashes of images and compares them to a database of hashes already identified and confirmed to be CSAM. If it finds a match, the image is immediately blocked by the service provider. This tool has enabled content providers to remove millions of illegal photographs from the Internet; helped convict child sexual offenders; and in some cases, helped law enforcement rescue potential victims before they were physically harmed. However, the tool does not employ facial recognition technology, nor can it identify a person or object in the image. PhotoDNA for Video breaks down a video into key frames and essentially creates hashes for those screenshots. In the same way that PhotoDNA can match an image that has been altered to avoid detection, PhotoDNA for Video can find child sexual exploitation content that has been edited or spliced into a video that might otherwise appear harmless.

[37] https://protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/

5 For ISPs, block access to URLs that are confirmed by the Cambodian authorities, international law enforcement or a registered Hotline such as the Internet Watch Foundation or ICMEC. This is provided for in the draft Child Protection Bill (Art. 119(5)), although the current wording refers to "indecent images", rather than all forms of CSAM (including for example, video content). ISPs should thus apply a strict application of the full definition of CSAM contained in these guidelines, consistent with the CRC Guidelines regarding the implementation of the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.

URL blocking should always be undertaken with caution, and only utilised on sites that have been independently confirmed to host or link to CSAM by a recognized international CSAM database holder.[38] This will prevent the inadvertent or otherwise blocking of access by children to legal information and content that may be erroneously blocked. By adhering to a common list of blacklisted URLS – which are available from partners such as the ICCAM databases, NCMEC or IWF – Cambodian companies will ensure that the actions they take do not infringe children's concurrent rights to information.

6 Establish Notice and Takedown procedures, that is, the detailed steps and processes to be followed where a report of CSAM or other illegal abusive content is received from law enforcement or an international agency. Notice and Takedown procedures generally only apply where CSAM is involved, or sexual abuse material, or other illegal content, as defined in law.

a. If content is hosted in Cambodia that may not be defined as illegal in the Cambodian Criminal Code but is illegal under the jurisdiction in which the digital technology company (usually social media companies) is registered, then the URL for the content will be entered into the ICCAM system by the CSAM reporting portal analyst (usually INHOPE or ICMEC) and a notification is automatically sent to law enforcement and the CSAM Hotline in Cambodia (currently operated by APLE). In all cases, Cambodian law enforcement is responsible for issuing the Notice to the Cambodian company on whose service or platform the content is registered. Requests may also be made from international law enforcement agencies through INTERPOL and EUROPOL, who then forward the information to the Cambodian law enforcement to issue a Notice and takedown order.

Any Takedown request (or Notice) originating in Cambodia, where CSAM has been identified in Cambodia, to an international social media or digital technology company, must come from the designated law enforcement agency, in Cambodia the Cyber Crime Unit. Any CSAM reported through the CSAM Hotline will also result in the Hotline forwarding a request to the Cyber Crime unit to issue a Takedown order.

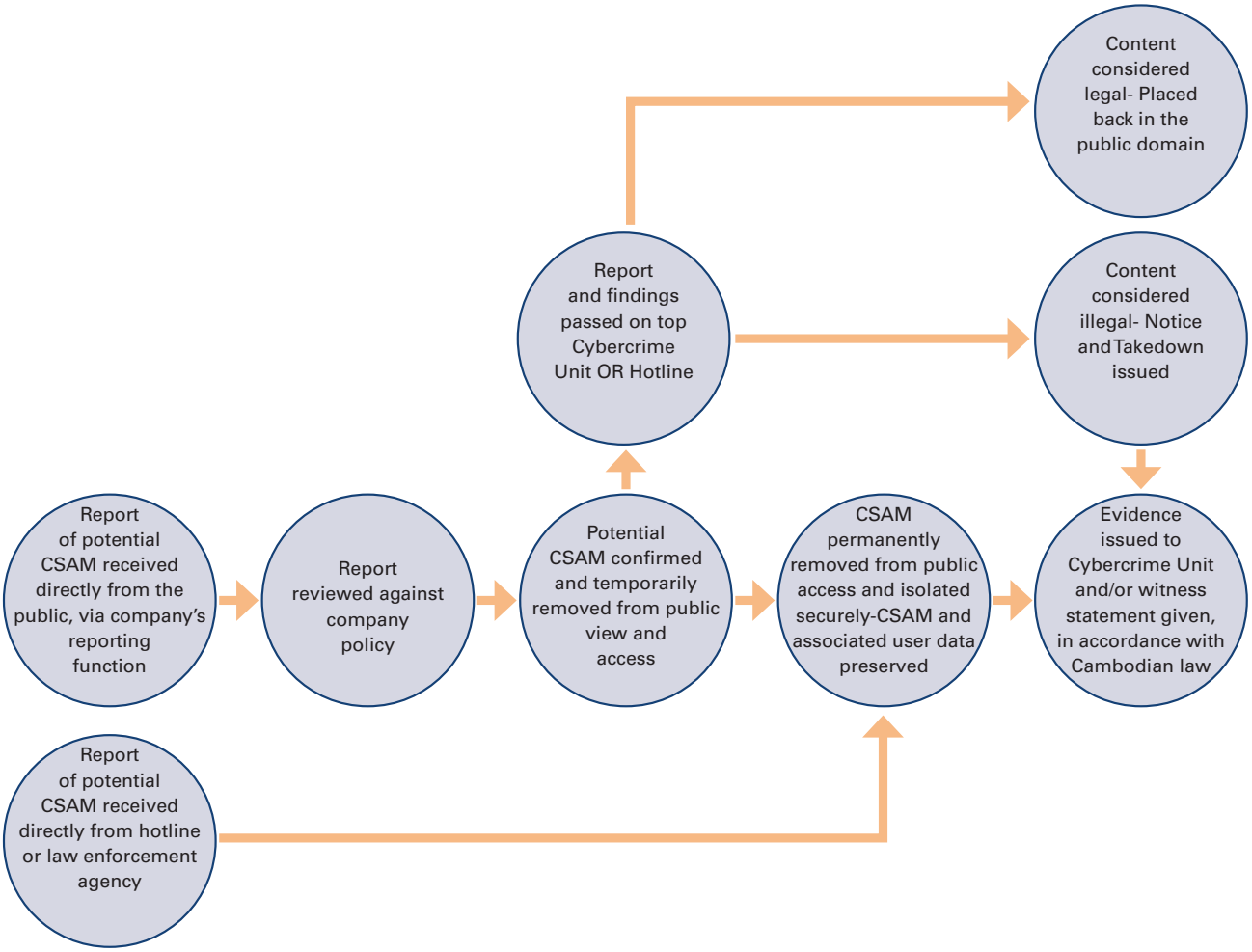
b. Notice and Takedowns can be initiated by Cambodian law enforcement based on information received from the public, or from a global digital technology company, ICMEC, IWF, or INHOPE, or INTERPOL or other State law enforcement. In such instances, the Cambodian authorities may be the conduit rather than the originator of the Notice.

[38] i.e. either the IWF or NICMEC CSAM image database, or the INTERPOL offender-based database.

c. A Cambodian company may receive a report of suspected CSAM or illegal content hosted on the companies server from a member of the public. The Cambodian company must then refer the report to the Cambodian law enforcement authorities (the Anti-Cyber-Crime Department) or the CSAM Hotline, who will assess or refer for assessment of the content using a process similar to that detailed in Figure 9, below. On receiving the initial report from the member of the public, the Cambodian company should isolate or otherwise remove the content from public access until it can be assessed.

d. By far the most common initiator of Notice and Takedown orders are those initiated by the global social media companies. These reports usually arise from their use of sophisticated CSAM detection tools, such as those described in point 4 above, and other screening and reporting measures. These reports are usually made in Cambodia directly to the Cambodian Anti Cyber-Crime Department.

Figure 9. CSAM reporting, assessment and take-down procedures[39]



7 Establish evidence preservation procedures to ensure that where CSAM material has been taken down, the necessary evidence is retained for a set time to assist in investigation and prosecution.

[39]UNICEF and GSMA, 2016, Notice and Takedown. Company policies and practices to remove online child sexual abuse material. Available online at https://www.gsma.com/mpoweryouth/resources/notice-and-takedown-company-policies-and-practices-to-remove-online-child-sexual-abuse-material/

a. It is important that these procedures do not allow for the retention of evidence, including any CSAM, for longer than is absolutely required for the purposes of investigation and prosecution, as the longer such content is retained, the greater risk it poses to the victim. While current Cambodian legislation, including the Criminal Code, does not currently provide for the length of time evidence is to be retained, the draft Cyber Crime law currently stipulates the retention of (any) data, on order of the government for up to 180 days. Failure to do so will result in fines or imprisonment, or both.

b. In addition to evidence retention, the company Notice and Takedown procedures should also define to whom disclosure can be made. This should ideally be made only to law enforcement (recognizing that a company may also report the content to the CSAM Hotline) or as necessary to respond to a legal process. Companies should establish a list of all personnel involved in handling CSAM or other classified content. As these individuals may be in direct contact with CSAM material, it is important that individuals are screened for any prior offences against children, and provision made for mental health support to this or these individual(s).

c. The evidence preservation procedures should also stipulate the process for the destruction of any illegal content following the mandatory retention period (see 7.a above).

BOX: A summary of roles and responsibilities relating to identification and response to CSAM

- The MPTC is responsible for coordinating the role and responsibilities of different agencies. Together with the National Regulator, the MPTC has oversight of industry in complying with its obligations.
- National Law Enforcement is responsible for investigating all cases of OCSEA hosted within Cambodia, or where the victim of perpetrator is located within Cambodia.
- In some instances, Cambodia law enforcement may receive notifications from INTERPOL or other international law enforcement body, and request they issue a Takedown Notice to the Cambodian company. A report may be received from an international INHOPE CSAM or ICMEC Hotline, and the Cambodia law enforcement will then issue the Takedown order.
- If Cambodia law enforcement are made aware of any CSAM through any other mechanism, they are responsible for reporting this content, with URL, to the ICMEC or CSAM Hotlines, as well as law enforcement to ensure that the relevant content is hashed and added to the CSAM database.
- Any digital technology company within Cambodia is obliged to act immediately on any Takedown Notice received from national law enforcement, and effect the takedown of the material, and preserve the material along with any user data.
- If a Cambodian digital technology company is made aware through any other mechanism, such as a direct report from a member of the public or a child, of potential CSAM, that content should be taken offline while it is reported to the Hotline, and assessed, and should it be deemed CSAM should be permanently removed by the company, and the material and all user data preserved.

8 Create referral pathways for victims into the formal child protection system. The digital technology company may be the first contact point for a child reporting abuse. It is important that in addition to recording and acting on the report of CSAM, other forms of OCSEA or any other form of digitally facilitated violence, the company provides a referral mechanism to a Helpline or another facility, with the child's consent, where children can speak to someone about their experience, and where they can if necessary be referred to the formal child protection system. This reflects the requirements in the Cambodian National Action Plan to end OCSEA, as well as the pending Child Protection Law.

It is important that companies do not themselves attempt to assess the risk or need of different reports for referral to the formal child protection system. Any referrals made to Helplines will be assessed by trained analyst or counsellors as to whether each case meets the criteria for referral to the formal protection system, where a full case assessment will be made. Notwithstanding this, ALL cases of CSAM that are reported to the CSAM Hotline will be assessed for referral.

Creating a safe and child-friendly digital environment

The digital technology industry in Cambodia has a critical role to play in creating safe online environments. This role is closely informed by the adoption of safety and privacy-by design codes, and the centering of child rights impact assessments. These should point to further practical steps that the digital technology industry can take in making sure that safe environments exist for children, as envisaged by the INSPIRE and MNR strategies and frameworks.

These processes should start with, and will be facilitated by, CRIA 's, safety-by-design and age-appropriate designs, as well as the provision of clear and easily understandable terms and conditions and acceptable use of policies, as discussed earlier.

> *"Where parental controls are used, they should be accompanied by very clear guidance on how they are to be used, and what the limitations of their use are. There is substantial evidence that parental controls are less effective for older children, as children quickly gain the technical skills to circumvent them (UNICEF East Asia and the Pacific and the Centre for Justice and Crime Prevention, 2020).*
>
> *Parental controls also have significant implications for a child's ability to develop further digital skills and capacities and serve as a barrier to the opportunities and benefits they could realise online, and so should always be appropriate to the developmental context of children (ITU, 2021).*

In some instances, and depending on the nature of the services provided, the provision of parental controls may be advised. Where parental controls are provided, they should be accompanied by clear guidance on how they are to be used, and what the limitations of their use are. There is substantial evidence that parental controls are less effective for older children, as children quickly gain the technical skills to circumvent them. Parental controls also have significant implications for a child's ability to develop further digital skills and capacities and serve as a barrier to

the opportunities and benefits they could realise online, and so should always be appropriate to the developmental context of children. In Cambodia, the use of parental controls may also be hampered by parents and caregivers own lack of digital skills.

Parental controls can be provided as a Value Added-Service to users, as a default option. This may be useful for consumers who have low levels of digital literacy and should always be accompanied by education and support for users that raise awareness of the limitations of these controls and the importance of using them within a broader package of support for young children, and when they cease to become effective.[40]

Companies should always ensure that opt-out services are easily available and advertised, and that privacy settings are set to private by default. This ensures that when children download new apps or software, their accounts and contacts are private, and they need to take the active steps to make their information public. This includes both viewing and receiving of messages or content from others, with default settings allowing only for contact from contacts or friends. These privacy settings should extend to location-related data, and the collection, processing and publishing of personal data, including browsing habits. Information on sharing of data and the purpose of data collection and data expiration, should also be provided in an easily accessible form.

Where content and online services and products are designed specifically for children, companies should undertake some level of moderation to ensure that unacceptable behaviour, as defined in the acceptable use or Terms and Conditions policies, are not breached. These should include:

- Posting unpleasant or threatening comments on someone's profile
- Setting up fake profiles or hate sites to humiliate or embarrass users
- Sending messages and attachments to humiliate a victim
- Hacking into someone else's account to send offensive messages to others
- Hacking into someone's account to steal messages or other content.[41]

> Children asked the private sector to empower children to easily access and adjust their privacy settings, and to guide parents and caregivers to guide children and young people about protecting their privacy and personal data online.
>
> *A Children's Call to Action. the ASEAN ICT Forum, November 2022*

As noted earlier, ensuring that there are clear reporting, help-seeking and safety centre portals that are easily visible and accessible, and are easily understood by children, on all devices with which children and parents might access the internet, is an important step in not only ensuring the CSAM and OCSEA is prevented and responded to, but also in ensuring that users feel and are safe using platforms and apps.

[40] As useful example of this can be found in package of services provided by AIS in Thailand

[41] Adapted from ITU, 2021

The private sector should also ensure that they clearly make visible on all their apps, websites and programmes how to use privacy settings and how to protect their personal data (see box). This should always be presented in a way that children can easily understand and follow, including children with disabilities. This should also be included in education and awareness raising, addressed in the following section.

Education and awareness

Education and awareness raising are central to the RPA and to the Cambodian Action Plan to prevent and respond to online child sexual exploitation 2021-2025 (Strategic Goal 6), as well as the Regional Plan of Action for the Protection of Children from All forms of Online Exploitation and Abuse (Focus Area 6). The Cambodian Digital Economy and Society Policy Framework 2021-2035 notes the importance of incorporating digital education into curriculums at all levels of the education system. Education and awareness are also reflected in both the MNR and the INSPIRE strategy. As noted in the Assessment Report on the Child Online Protection in the Cambodian Technology Industry, this is one area in which many Cambodian tech and ICT companies are active. All technology companies in Cambodia have an important role to play in supporting the development of digital skills and capacities amongst children, parents and teachers. Each of these target audiences demands tailored messages based on their roles, responsibilities and capacities, which may in turn vary depending on their location and developmental context.

While digital literacy, media literacy, online safety and prevention education are fundamental to the safety and wellbeing of children online, and to their ability to fully realise the wealth of opportunities and benefits that being online presents, **the responsibility should never be placed on children for their own safety, when the devices, apps, platforms and other digital services that they use are inadequately designed for their safety and privacy.** That means that while supporting education and awareness raising are key areas of engagement for digital technology companies in Cambodia, this can never be done instead of, or expected to replace business practices, products and services that do not place children at the centre of their design and delivery or compensate for the lack of this centering of children.

Digital technology companies in Cambodia should ensure that education and awareness raising are based on evidence of what works in raising awareness and education. There is a growing body of evidence on what works in supporting children online through education and awareness raising, as well as, equally important, what does not work. This evidence should form the basis of company's outreach, education and awareness programming at all times (see text box below).

Education programmes for children and parents should be tailored to the developmental contexts and children's developmental stages, with appropriate messages relating to appropriate use of digital devices and technology. These should align with the table provided in appendix 3 of these Guidelines.

Digital technology companies in Cambodia should explore ways of supporting existing Social and Behavioural change programmes rather than stand-alone ad-hoc awareness and education interventions (including those focusing on sexual and reproductive health in schools) and

integrating online safety messaging relating to the prevention of OCSEA into those programmes. Recent evidence points to the importance of integrating education to prevent OCSEA into existing programmes that work, both through schools and other bodies.[42] This is an important area where the tech industry in Cambodia, from connectivity to content providers, can support developing the capacity and resilience of children to successfully navigate the risks they might encounter online, as well as raising awareness of the practical tools that children (and parents) can use.

The industry should also ensure that parents and caregivers, as well as teachers, are aware of appropriate services, apps and platforms for children of different ages, and the various reporting and information centres relating to each of these. Where relevant, education material should always be accompanied with direct links to the reporting and trust and safety centres of all apps and platforms, and to Helplines, including the APLE Hotline and Helpline, and on how to report misuse or abuse.

One practical way that the telecommunications and ISP providers within Cambodia can foster greater awareness raising, including through social and behavioural change and evidence-based messaging, is to **work with the MPTC and Cambodian Government more broadly to provide credits specifically for awareness and education messaging relating to online safety and child online protection on their platforms.**

Education and awareness programmes should be evaluated for content revisions at regular intervals, based on research and documented evidence. Messaging programmes, awareness raising initiatives, and education programmes should all be assessed for knowledge uptake and retention, rather than simple awareness measures. This means that each intervention should be evaluated by determining the degree to which the children (and where relevant adults) who participated in the initiatives are able to remember and practice the skills that they have learnt, over time. Such assessments are critical to improving messaging, adapting to the changing needs and situations that children face, and to ensure that they are child or stakeholder friendly. The delivery of awareness interventions and education programming are only as useful as the long-term impact that they achieve. As part of ongoing transparency to the protection of children's rights, and public commitment to promoting safe digital environments, and equipping children with the skills that they require to safely and productively use products and services, companies should also make the results of these evaluations and assessments public.[43]

The digital technology industry in Cambodia also has an important role to play in supporting evidence-generation within Cambodia. Cambodia now has an established baseline relating to OCSEA and other forms of technology-facilitated violence, in the Disrupting Harms Study Cambodia.[44] However, there is need for the expanding of this evidence to include evidence of Cambodian-specific interventions, and the effectiveness of education and awareness programming as implemented in Cambodia. Further, as new technology is introduced, EdTech is rolled out, and AI and machine learning becomes more embedded in everyday life in Cambodia, more research on risks, potential harms, and how these can be mitigated to maximise the opportunities and benefits that these can bring, should be conducted. The digital technology industry within Cambodia is central to this process.

[42] WHO, 2022

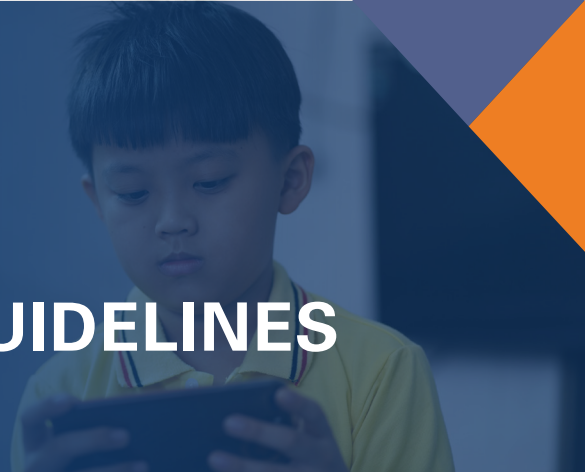
[43] A useful guide for evaluating online safety initiatives is available here: UNICEF East Asia and the Pacific and Young and Resilient Research Centre, Evaluating Online Safety Initiatives: Building the evidence base on what works to keep children safe online. UNICEF, Bangkok, 2022.

[44] Kardefelt Winther, Daniel (2022). Disrupting Harm in Cambodia: Evidence on online child sexual exploitation and abuse, Innocenti Research Report

BOX: Dispelling some myths: Important things for Industry to know from what the evidence tells

- ✗ *Myth: Most CSAM circulates on the dark web.*
- ✓ *Based on CSAM identified by Project Arachnid, almost all (97%) of CSAM is physically hosted on the 'clear' web, rather than the dark web (C3P, 2021).*
- ✗ *Myth: Most OCSEA is perpetrated by strangers (what is known as the "stranger danger").*
- ✓ *While risks, particularly sexual contact risks, from people unknown to children often pose the risk of the most severe harm, children are far more likely to experience risks from people known to them, ranging from family (close and extended family) to friends or other community members (WHO, 2022). In Cambodia, only 1 in 5 instances of OCSEA were perpetrated by someone unknown to the victim (UNICEF, 2022, Disrupting Harms Cambodia)*
- ✗ *Myth: OCSEA is the most common form of harm experienced by children online, and the most severe.*
- ✓ *Risks, and potential harms, should not be graded for severity, as experiences that many perceive as 'less serious', such as teasing or other forms of cyber-bullying, can result in the most severe harms for children, particularly when experienced over time.*

Why is it important for Industry to be aware of these myths? The digital technology industry in Cambodia, as in other country, often invests in raising awareness and building the capacity of children, parents and teachers as part of their educational and awareness work. If these messages and campaigns are to be effective, it is important that they incorporate evidence-based messages and lessons, rather than reflecting common, but incorrect, messages and lessons. There is a growing body of evidence and guidance on what works, that should inform the content and delivery of awareness raising and educational programmes. These should be regularly evaluated on the basis of new evidence and ongoing research.



APPENDIX 1: OVERVIEW OF THE ITU GUIDELINES ON COP

The International Telecommunications Union (ITU), together with UNICEF have developed specific guidelines for the digital technology industry globally, adopting a child rights approach, that provides a roadmap for the private tech industry to ensure and promote child online protection. Importantly, these are not general guidelines but are targeted to the needs and operations of the technology and telecommunications industry specifically. Note that these Guidelines for the Cambodian Tech Industry have been heavily informed by these global guidelines to ensure alignment.

These guidelines outline five specific areas in which industry can protect and promote child rights to ensure the safety and protection of children:

1. Integrate child rights into all appropriate corporate policies and management processes. This requires examining each company's own internal policies and processes to ensure that the best-interest of children is at the centre of decisions, and that all internal processes are established to protect this wellbeing and children's rights, and to act internally, and with accountability, when these rights are jeopardized or violated.

2. Develop standard processes to handle child sexual abuse material (CSAM). Child sexual abuse material is now primarily produced, hosted, and transmitted, using digital technology. Each company, regardless of the service or products it delivers, should have internal and external policies and protocols to detect, identify, refer and delete CSAM material from corporate networks, URLs, services or products, as well as to collaborate with national and international law enforcement and civil society in dealing with CSAM.

3. Create a safer and age-appropriate online environment. The products and services that the private sector should always take into account the different risks that children encounter online – content, contact, conduct and contract – and take necessary steps to create products that are "easy to use, safe and private by design and are age-appropriate to all users, including children."[45]

4. Educating children, caregivers and educators about children's safety online and the responsible use of ICTs. While companies play a critical role in ensuring that children's experiences online, and their use of technology, is safe, parents/caregivers, teachers and other responsible adults in children's lives also play an important role in fostering the skills that children require to stay safe, as well as in taking specific measures that are age-appropriate. Companies thus have an important role to play in educating and empowering parents and teachers in their role in keeping children safe, in how to use and what the limits are of, tools such as parental monitoring tools, and what is appropriate tech use and online activities at different ages in any child's development stages.

[45] International Telecommunications Industry. (2020). p 8

5 **Promoting digital technology as a mode for increasing civic engagement.** Article 13 of the Convention on the Rights of the Child enshrines children's right to express and participation, through all mediums of their choice. This is further reflected in GC.25 which notes States responsibilities to protect children's right to participation and to expression, including through the use of digital technology and the internet. It is important that companies ensure that the products and services that they develop, and the measures that they take to protect children online, do not infringe on the same children's right to express themselves through technology and the internet, or to participate in the wealth of activities and opportunities that being online present. As importantly, companies can invest in promoting children's participation, along with the required skills to participate equitably, in civic life.

Within each of these areas, the Guidelines offer more concrete actions that industry can take in both ensuring children's right broadly, and in preventing and responding to online violence and exploitation against children that may occur over their platforms, products and services.

APPENDIX 2: AGE AND DEVELOPMENTAL STAGES

Age/Stage	Key considerations
0-5 **Pre-literate and early literacy**	There is relatively little evidence on the understanding of the digital environment of children in this age range, particularly for 0-3 years old. However anecdotal evidence suggests that significant numbers of children are online from the earliest of ages and that any understanding and awareness of online risks that have children within this age range is very limited. At age 3-5 children start to develop the ability to 'put themselves in others shoes', but are easily fooled by appearances. They are developing friendships, although peer pressure is relatively low and parental or family guidance or influence is key. They are learning to follow clear and simple rules but are unlikely to have the cognitive ability to understand or follow more nuanced rules or instructions, or to make anything but the simplest of decisions. They have limited capacity for self-control or ability to manage their own time online. They are pre-dominantly engaged in adult-guided activities, playing within 'walled' environments, or watching video streams. Children in this age range are less likely than older children to have their own device, although significant numbers do, and often play on their parents' devices which may or may not be set up with child specific profiles. They may use connected toys (such as talking teddies or dolls) and may also mimic parents' use of voice activated devices such as 'home hubs'. Children within this age range are pre-literate or in the earliest stages of literacy, so text-based information is of very limited use in communicating with them. UK children in this age range cannot provide their own consent to the processing of their personal data in the context of an online service offered directly to a child (by virtue of Article 8(1) of the GDPR and s9 of the DPA 2018). So if you wish to rely on consent as your lawful basis for processing their personal data you need parental consent.

6-9

Core primary school years

Children in this age range are more likely than younger children to have their own device (such as a tablet), although use of parents' devices is still common. They are increasingly using devices independently, with or without the benefit of child specific profiles. Connected toys are popular and they may engage enthusiastically with voice activated devices such as home hubs.

Children in this age range often prefer online gaming and creative based activities, and video streaming services remain popular. Children may be experimenting with social media use, either through social aspects of online games, through their parents' social media accounts or by setting up their own social media accounts. They may relate to and be influenced by online vloggers, particularly those within a similar age range.

They are likely to be absorbing messages from school about online safety and the digital environment, and be developing a basic understanding of privacy concepts and some of the more obvious online risks. They are unlikely however to have a clear understanding of the many ways in which their personal data may be used or of any less direct or obvious risks that their online behaviour may expose them to.

The need to fit in with their peer group becomes more important so they may be more susceptible to peer pressure. However home and family still tends to be the strongest influencer. They still tend to comply with clear messages or rules from home and school, but if risks aren't explained clearly then they may fill the gap with their own explanations or come up with protective strategies that aren't as effective as they think they are.

Literacy levels can vary considerably and ability or willingness to engage with written materials cannot be assumed.

UK children in this age range cannot provide their own consent to the processing of their personal data in the context of an online service offered directly to a child (by virtue of Article 8(1) of the GDPR and s9 of the DPA 2018). So if you wish to rely on consent as your lawful basis for processing their personal data you need parental consent.

10-12

Transition years

This is a key age range in which children's online activity is likely to change significantly. The transition, or anticipated transition, from primary school to high school means that children are much more likely to have their own personal device (pre-dominantly smartphones).

There is also likely to be a shift towards use of the online environment to explore and develop self-identity and relationships, expand and stay in contact with their peer group, and 'fit in' socially. This may lead to an increased use of social networking functions or services by children within this age range, an increased susceptibility to peer pressure, branding and online 'influencers', and an increase in risk taking behaviours. Self-esteem may fall as children compare themselves to others and strive to present an acceptable version of themselves online and the 'fear of missing out' may become a concern.

Online gaming and video and music streaming services are also popular. Children may feel pressurised into playing online games when their friends are playing, again for fear of missing out.

Attitudes towards parental rules, authority and involvement in their online activity may vary considerably, with some children relatively accepting of this and others seeking higher levels of autonomy. However parents and family still tend to be the main source of influence for children in this age range.

Children in this age range are moving towards more adult ways of thinking but may have limited capacity to think beyond immediate consequences, be particularly susceptible to reward based systems, and tend towards impulsive behaviours. Parental or other support therefore still tends to be needed, if not always desired. It may however need to be offered or encouraged in a less directive way than for younger children.

Children in this age range are developing a better understanding of how the online environment operates, but are still unlikely to be aware of less obvious uses of their personal data.

Although children in this age range are likely to have more developed literacy skills they may still prefer media such as video content instead.

12 is the age at which, under s208 of the DPA 2018, children in Scotland are presumed (unless the contrary is shown) to be of sufficient age and maturity to have a general understanding of what it means to exercise their data protection rights. There is no such provision for children in the rest of the UK, although this may be considered a useful reference point.

UK children in this age range cannot provide their own consent to the processing of their personal data in the context of an online service offered directly to a child (by virtue of Article 8(1) of the GDPR and s9 of the DPA 2018). So if you wish to rely on consent as your lawful basis for processing their personal data you need parental consent.

13-15

Early teens

In this age range the need for identification with their own peer group, and exploration of identity and relationships increases further and children are likely to seek greater levels of independence and autonomy. They may reject or distance themselves from the values of their parents or seek to actively flaunt parental or online rules. The use of new services that parents aren't aware of or don't use is popular as is the use of language that parents may not easily understand. However, despite this, family remains a key influence on children within this age range. The use of social media functions and applications is widespread although gaming and video and music streaming services are also popular. Again children may seek to emulate online 'influencers' or vloggers at this stage in their development.

Children of this age may still look to parents to assist if they encounter problems online, but some may be reluctant to do so due to concerns about their parents' reaction to their online activity.

Developmentally they may tend toward idealised or polarised thinking and be susceptible to negative comparison of themselves with others. They may overestimate their own ability to cope with risks and challenges arising from online behaviour and relationships and may benefit from signposting towards sources of support, including but not limited to parental support.

Literacy skills are likely to be more developed but they may still benefit from a choice of media.

13 is the age at which children in the UK are able to provide their own consent to processing, if you relying on consent as your lawful basis for processing in the context of offering an online service directly to a child (by virtue of Article 8(1) of the GDPR and s9 of the DPA 2018).

16-17

Approaching adulthood

By this age many children have developed reasonably robust online skills, coping strategies and resilience. However they are still developing cognitively and emotionally and should not be expected to have the same resilience, experience or appreciation of the long term consequences of their online actions as adults may have.

Technical knowledge and capabilities may be better developed than their emotional literacy or their ability to handle complex personal relationships. Their capacity to engage in long term thinking is still developing and they may still tend towards risk taking or impulsive behaviours and be susceptible to reward based systems.

Parental support is more likely to be viewed as one option that they may or may not wish to use, rather than as the preferred or only option, and they expect a reasonable level of autonomy. Signposting to other sources of support in addition to parental support is important.

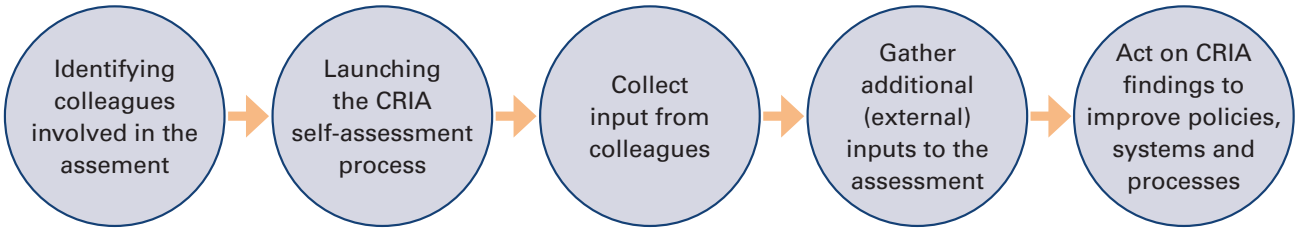
By virtue of Article 8(1) of the GDPR and s9 of the DPA 2018, if you are relying on consent as your lawful basis for processing in the context of offering an online service directly to a child, UK children in this age range can provide their own consent to the processing of their personal data.

Source: Information Commissioners Office, 2021, Age-appropriate Design: A Code of practice for online services. ICO: London

APPENDIX 3: STEPS IN A CHILD RIGHTS IMPACT ASSESSMENT

The UNICEF Mobile Operators – Child Rights Impact Self-Assessment Tool provides a five-step process for undertaking a child rights assessment. The scale of each step can be adapted to different size organizations, but none of the steps should be sacrificed in this adaptation. The tool provides guidance on expectations and processes in seven areas of particular relevance to mobile operators: corporate social responsibility and sustainability; children in the digital environment, human resources, products sales and marketing; procurement; network operations; and security.

Figure. Carrying out a CRIA self-assessment



An example of expectations in the area of children in the digital environment is provided in the table below. In each area, specific steps can be taken to meet the expectations, in line with the principles tools and mechanisms outlined in the Guidelines.

Area	Expectation
Policy on children's rights in the digital environment	The company has defined a company-wide policy, principles, standard or code of conduct that addresses children's rights online, that takes a zero-tolerance approach to CSAM and other forms of OCSEA, and these are applied in all of the company's local operations.
Communication about the company policy on product and service misuse	The company's terms and conditions of service provision clearly communicate its policies and procedures regarding misuse of its products or services to exploit or abuse children.
Safety by design	The company takes proactive steps to assess the positive and negative impact on children's rights across different age groups in the design, development and introduction of new digital products and services.

Preventing access, sharing, storage of CSAM	The company has in place measures to restrict access, sharing and storing of CSAM that are consistent with local laws and international standards, and these restrictions are strictly limited to CSAM.
Notice and takedown procedures and identification of CSAM	If the company hosts content, or sells content storage services on the cloud provided by a third party, it has 'notice and takedown' processes in place or ensures that the third party partner does.
Supporting mechanisms to report CSAM	The company works with relevant partners to promote and provide free access to hotlines to report CSAM.
Measures to protect children from inappropriate content	Appropriate content filtering solutions and/or parental control tools are offered free of charge for the company's mobile and fixed internet services.
Promoting resilience and safe internet use	The company provides advice to children, parents, caregivers, and teachers on how technologies work and guidance to understand the actions they can take to stay safe online.
Supporting child helplines	The company promotes child helplines and other services that enable children to seek support in the case of concerns, abuse or exploitation both online and offline.

APPENDIX 4:
COP COMPLIANCE CHECKLIST

Using the COP Compliance checklist.

1. The below compliance checklist can be used as the basis of transparency reporting on an annual basis or otherwise determined interval, to reflect actions that companies of different sizes have taken to address their obligations and commitment to keeping children safe online.
2. Items marked as **bold** should be considered minimum expectations and requirements, and all companies should assess themselves and be able to report on steps taken towards achieving these outcomes. Those marked in italics are those steps that companies of all sizes should work towards achieving, recognizing that particularly for small and micro-enterprises, including start-ups, these may take time to achieve.
3. Where any particular area is not relevant to the services or products provided by a company, the company may mark that item as Not Applicable (N/A). However, blanket use of this response is strongly discouraged, and companies should be able to reflect why these items are not relevant to their business or service.
4. Each of these steps, while action and outcome oriented, also reflect underlying principles and commitment to respecting and institutionalizing the rights of children, recognizing their evolving and changing capacities, into all aspects of business. Like the Guidelines themselves, this checklist should be viewed as a living document, and will be updated as digital technology evolves, and as the risks, and the experience of risks, that children face online evolve accordingly, and as digital technology itself and the use of new and emerging technology to protect children's rights, evolve.
5. The below list does not preclude companies from reporting on additional measures, outcomes or principles they have adopted to protect children's rights and their safety and wellbeing online.

Area		Action	Compliant			
			Partially	Yes	No	N/A
Child Rights Impact Assessment	1	Company has undertaken an internal child rights impact assessment	☐	☐	☐	☐
	2	*Company has made results of the CRIA publicly available*	☐	☐	☐	☐
	3	Company has established or appointed an internal child rights officer/office	☐	☐	☐	☐
	4	Company can show how it has acted to address results of CRIA (ask company for concrete examples)	☐	☐	☐	☐
	5	Company can show it has specifically assessed the potential safety impact of its products or services (ask company for concrete examples)	☐	☐	☐	☐
	6	Company has established a reporting mechanism for grievances relating to violations of users' human rights (incl. child rights)	☐	☐	☐	☐
	7	Company has (updated) child safeguarding policy in place	☐	☐	☐	☐
	8	Employees are aware of policies and where to report any child safeguarding concerns	☐	☐	☐	☐
	9	*Company has conducted an "audit" of user privacy mechanisms and data protection systems*	☐	☐	☐	☐
	10	*Company has made results of data privacy and protection audit publicly available*	☐	☐	☐	☐
Safety and privacy by design	11	Company has taken steps to ensure users data privacy and protection, including data minimisation, purpose limitation, storage limitation and security	☐	☐	☐	☐
	12	Company ensures data minimisation across services	☐	☐	☐	☐
	13	Company ensures data purpose limitation across services	☐	☐	☐	☐
	14	Company ensures storage limitation across services	☐	☐	☐	☐
	15	Company ensures data security across services	☐	☐	☐	☐
	16	*Company has taken visible steps to accurately assess and ensure the age of it's potential user base*	☐	☐	☐	☐
	17	Company clearly informs users on the collection and use of data, and the purpose for which all data is collected	☐	☐	☐	☐
	18	Company data policy and information is easily accessible and comprehensible by users of all ages	☐	☐	☐	☐

Child Sexual Abuse Material (CSAM)	19	Company has (updated) code of conduct place that specifies zero-tolerance approach to CSAM, OCSEA and all forms of technology-facilitated violence, and related penalties	☐	☐	☐	☐
	20	Company publicises its terms and conditions and/or Acceptable Use policy that explicitly prohibits any form of CSAM or OCSEA	☐	☐	☐	☐
	21	*Terms and Conditions and Acceptable Use policy is available in language that is readily acceptable and understood by children, people with disabilities, and parents or caregivers who may have limited digital literacy.*	☐	☐	☐	☐
	22	Company has a CSAM reporting facility in place (may be a functioning link to the CSAM Hotline, IWF or NCMEC reporting portal)	☐	☐	☐	☐
	23	Reporting Portal/link (above) is easily accessible and usable by children and those with limited digital literacy skills	☐	☐	☐	☐
	24	*Company has screened all those who may work with Notice and Takedown Orders, or otherwise be involved in the identification of CSAM, against criminal records (and sexual offenders register) (note this may be a single individual, or a team of designated individuals, depending on size of company)*	☐	☐	☐	☐
	25	Company has a demonstrable relationship with the Internet CSAM Hotline	☐	☐	☐	☐
	26	Company keeps records of number of reports made and actioned, and results of all reports	☐	☐	☐	☐
	27	*Optional (for MO and ISPs and other content service providers): Company subscribes to automated CSAM detection software*	☐	☐	☐	☐
	28	*If Company uses any URL blocking or filtering software, Company ONLY blocks those URLs identified by ICCAM, NICMEC, IWF data base.*	☐	☐	☐	☐
	29	Company has a documented internal Notice and Takedown procedure/protocol, and evidence retention policy	☐	☐	☐	☐
	30	If Company has evidence retention policy, company specifies process for destruction of data, use information and CSAM content AFTER designated retention period	☐	☐	☐	☐
	31	Company can identify designated reporting process for CSAM (reporting to Cyber Crime Unit)	☐	☐	☐	☐
	32	Company can provide correct process and referral mechanism to the Cambodian child protection system (Helpline or MoSVY)	☐	☐	☐	☐

Safe Online environment	33	If Company's services may be used or accessed by children, company has taken safety, privacy and age-appropriate design into consideration	☐	☐	☐	☐
	34	*If Company's services are specifically targeted towards children, then in addition to the above, company has put in place some form of age-appropriate moderation system that does not infringe on children's evolving rights to privacy, or access to information or participation.*	☐	☐	☐	☐
	35	If parental control measures are provided, or promoted, the Company explicitly makes clear what the limitations of these parental control measures are, and how to use them correctly	☐	☐	☐	☐
	36	Company provides privacy by default and easily accessible opt-out options.	☐	☐	☐	☐
Education and awareness	37	*Company is engaged in providing digital literacy programming*	☐	☐	☐	☐
	38	*Company is engaged in providing media literacy programming*	☐	☐	☐	☐
	39	*Company supports or directly offers prevention education or social and behavioural change programming*	☐	☐	☐	☐
	40	*Company partners with non-technology companies, NGOs and government to offer any of the above programmes*	☐	☐	☐	☐
	41	*Company supports research and evidence generation relating to technology-facilitated violence and online safety.*	☐	☐	☐	☐
	42	*Company undertakes R&D to develop innovative technological solutions to OCSEA and CSAM*	☐	☐	☐	☐

ADDITIONAL RESOURCES

ITU/UNICEF Guidelines for Industry on Child Online Protection: UNICEF-ITU guidelines for Industry on Child Online Protection ;

UNICEF's Child Rights and Business Principles: Child Rights and Business Principles

Global Child Forum's Child Rights Due Diligence Tool to implement a Child Rights perspective: Global Child Forum Child Rights Due Diligence Tool to implement a Child Rights Perspective,

Voluntary Principles to counter online child sexual exploitation and abuse: https://www.gov.uk/government/publications/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse

UNICEF's MO-CRIA: Child Rights Impact Self-Assessment Tool for Mobile Operators (2nd Ed): https://www.unicef.org/reports/mo-cria-child-rights-impact-self-assessment-tool-mobile-operators

Digital Future's Commission, Child Rights Impact Assessment: https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf

Broadband Commission for Sustainable Development: Working Group on Child Online Safety: https://broadbandcommission.org/working-groups/child-safety-online-2019/

Internet Watch Foundation CSAM reporting portal

Stop NCII portal (non-consensual intimate image abuse)

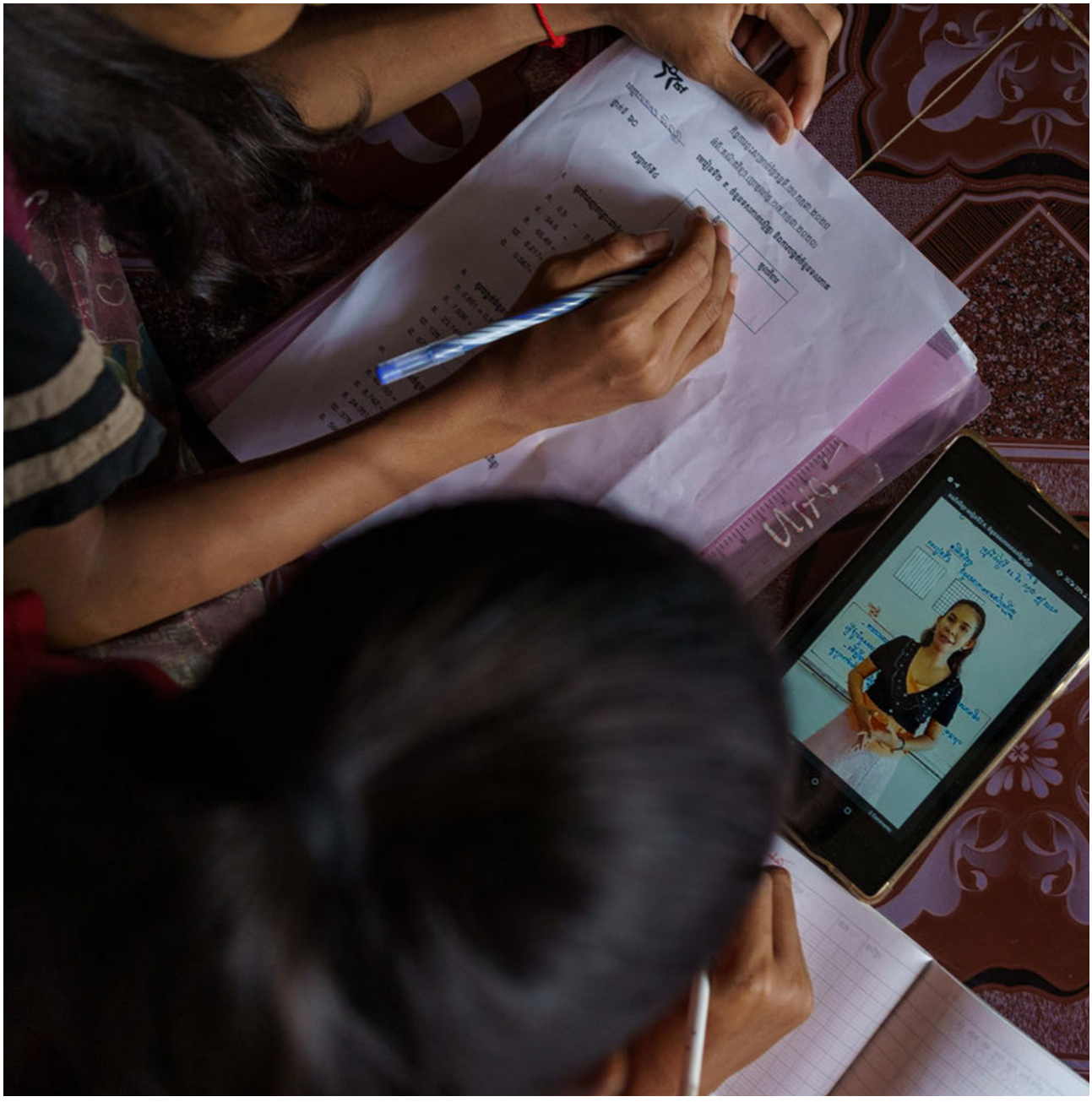
INHOPE Notice and Takedown Procedures: https://inhope.org/EN/articles/a-deep-dive-into-notice-and-takedown

Tech Coalition: https://www.technologycoalition.org/

Digital Trust and Safety Partnership: https://dtspartnership.org/

Thorn's AI-Driven CSAM detection and removal tool: https://safer.io/about/

Microsoft PhotoDNA: https://www.microsoft.com/en-us/photodna



Ministry of Posts and Telecommunications No.13, Preah Monivong Blvd,
Sangkat Srah Chak, Doun Penh, Phnom Penh, Cambodia

unicef
for every child

UNICEF Cambodia Country Office
5th floor, Exchange Square, Bldg. No. 19&20, Street 106 Sangkat Wat
Phnom, Phnom Penh, Cambodia