Ministry of Post and Telecommunications

CAMBODIAN CHILD ONLINE PROTECTION GUIDELINES FOR THE DIGITAL TECHNOLOGY INDUSTRY

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

1. INTRODUCTION

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 sexual exploitation and other forms of violence against children.[1] 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[2], and is embedded in the National Action Plan to Prevent and Respond to Online Child Sexual Exploitation in Cambodia 2021-2025. This document provides a summary of the full guidelines and should be read on conjunction with the full Guideline document.

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.

The Guidelines are framed within the Children's Rights and Business Principles (CRBP) developed by UNICEF, the Global Compact and Save the Children, and endorsed by industry, as well as the 2021 UNCRC General Comment No. 25 on Children's Rights in the Digital Environment.

The General Comment No.25 of the Committee on the Rights of the Child details the obligations of all State parties to the Convention on the Rights of the Child to ensure that children's rights apply equally within the digital environment, to their application in the offline space. The General Comment requires states to (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

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 Unpublished research report

[2] 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

their rights to privacy and protection, and to provide children, parents and caregivers with prompt and effective remedies. 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, and to take steps to monitor, prevent and act against business who infringe on the rights of children as enshrined in the Convention.[3]

This explicitly places a responsibility on all technology and telecommunications industries 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 business violate the rights of children. These Guidelines are one measure taken by the MPTC towards the institution of this responsibility on the Kingdom of Cambodia, as a party to the Convention on the Rights of the Child.

The Guidelines are consistent and aligned with the 2021 Regional Plan of Action (RPA) for the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN, as well as various national policies, including the 2023 CNCC National Guidelines on Online Child Protection explicitly notes the role of the digital technology industry in COP, and Chapter Six of the Draft Law on Child Protection (February 2023 draft). While these Guidelines are intended primarily for the Cambodian digital technology sector, they are also 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.

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 (MNR) to End Online Child Sexual Exploitation and Abuse, the INSPIRE Strategies to End Violence Against Children (INSPIRE), and the Regional Plan of Action (RPA) 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.

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

- The ASEAN RPA has seven 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.

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.

1.1 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.

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

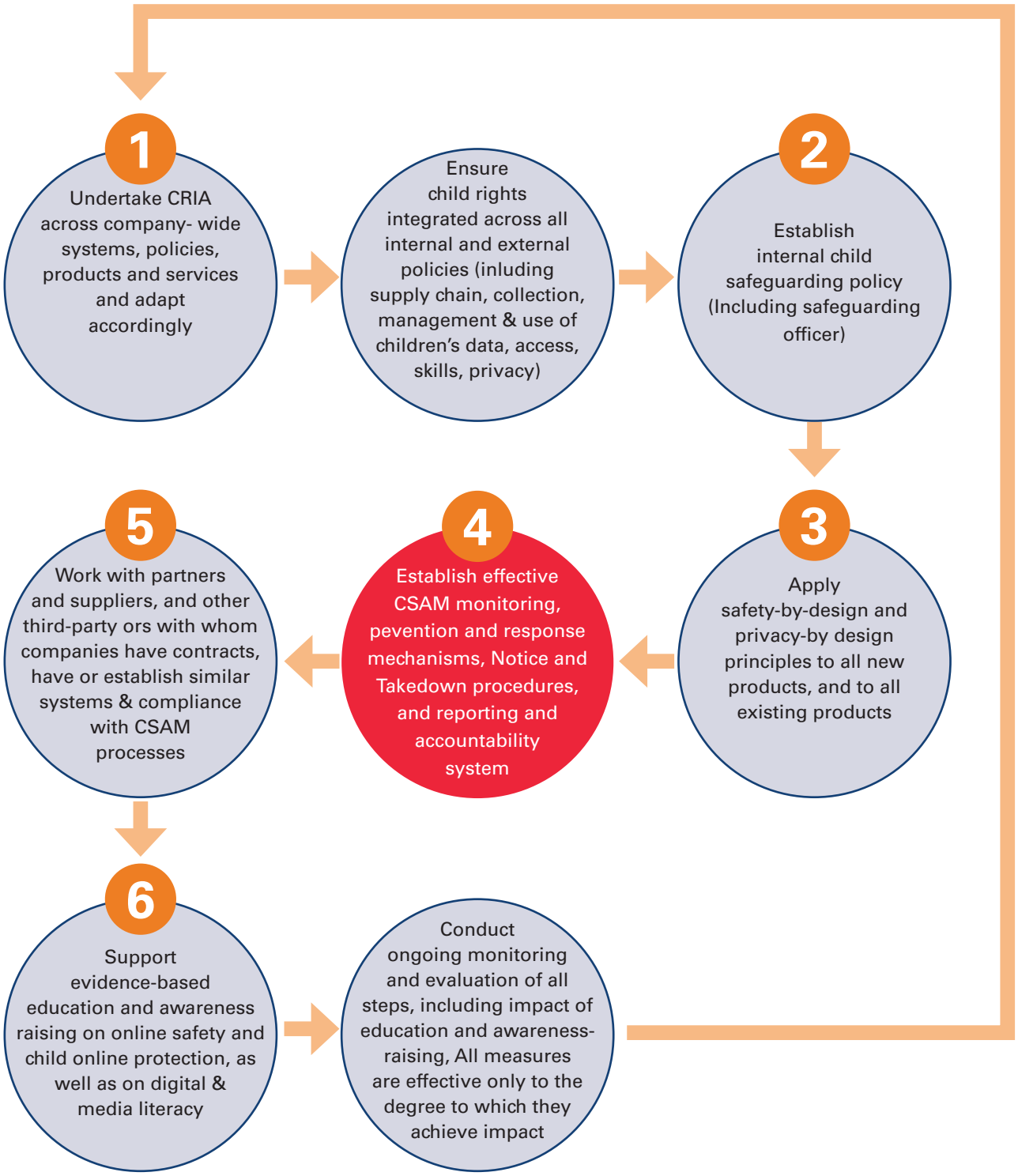
The protection of the rights of subscribers, in general, are addressed through a number of existing legal texts. The rights of subscribers to telecommunication (including information) services to privacy, security and safety are protected under Article 65 of the Law on Telecommunications (2015) of the Kingdom of Cambodia. The Law also notes the rights of subscribers to participate in, and be consulted, on all aspects of policy development related to telecommunications policy. The obligations of the Operators in relation to these rights are more explicitly noted in Sub-decree No 110 on the ICT licensing Regine, which notes in Article 27 that a specific burden of responsibility rests on all those providing ICT services and products to:

a. Safeguard private information, security and safety on the use of ICT services (27:f);
b. Provide operations and services with honesty, freedom, equality and efficiency (27:g);
c. Practice according to advice and guidance from the Ministry of Post and Telecommunication (27:h);
d. Forbid illegal businesses or conduct on or through their services or products (27:i);
e. And undertake other duties established by the MPTC (27:j).

These Guidelines are framed within the scope of Article 27:j, which explicitly notes the responsibility of all telecommunications operators and those providing products and services within the ICRT industry to act on the duties established for the sector by the MPTC.

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. These Guidelines 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 are 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, as well as with the obligations and procedures relating to those conducting any form of E-commerce within Cambodia, as defined in the Law on Electronic Commerce (2019) of the Kingdome of Cambodia. This includes 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 guidelines 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 the common goal of a safe digital world for children.

2. PRACTICAL STEPS REQUIRED OF THE DIGITAL TECHNOLOGY SECTOR IN CAMBODIA



While the different mechanisms included in these guidelines 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 will also play a role in providing specialized support to smaller companies and start-ups in realising their 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 their differing capacities, and so recognize the scope of these assessments may vary. Note that some aspects of these different steps may overlap, and companies asked to assess and report on the same aspects across steps, for example, the appointment of a dedicated person to deal with child protection or safety. There is no need to report multiple times on the same aspects, as long as no change in position has occurred in the interim between different assessments or steps.

Transparency is a critical tool in accountability and can increase the public's confidence and trust in products and services. 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.[4] These reports can draw on the self-assessment checklist provided in the full Guidelines for key indicators and metrics on which they can report.

2.1 Child Rights Impact Assessments (CRIA)

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. 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. 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.[5] While this was developed specifically for mobile operators, it can easily be adapted to different types of businesses within the digital technology sector. Where companies can demonstrate recent completion of CRIAs, these do not need to be repeated.

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

[5] UNICEF, 2021, MO-CRIA: Child Rights Impact Self-assessment Tool for Mobile Operators, UNICEF, New York).

2.2 Formulate and implement internal child safeguarding policies and procedures

Businesses should all formulate and implement **internal child safeguarding policies and procedures,** that are applied across all departments and divisions within the company, intended to protect employees and children from harm, including the careful vetting of any employees who might encounter CSAM. 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, and how and where to confidentially report any breaches or suspicions of breaches. These safeguarding policies should be formally incorporated into their bylaws or internal policies and procedures.

2.3 Safety by design Principle

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.

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."[6] Cambodian companies should adopt and commit to using safety-by-design principles in all new products and services. Several examples of safety-by-design principles have been developed with the support and commitment of digital technology companies around the world and can provide guidance on how to integrate safety by design into everyday operations. One example can be found here in the e-safety Commissioner's safety-by-design self-assessment tools. It is important that children's experiences, and their participation, inform the development of these safety-by-design principles, to ensure that their concerns are directly reflected in the approaches adopted by companies operating in Cambodia.

Related to this, ensure age-appropriate design for the target audience, using the developmental and evolving capacity of children as a guide (see appendix). **Age-appropriate design 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,** into the design and development of any new product or service. This ensures that from the outset of a product development, the impact

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

of that product or service on children of different ages is considered. Simply, by agreeing to and adopting age-appropriate design codes, companies 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.

This includes the collection and use of children's 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. Special measures to be taken to ensure that children's rights are protected include data minimisation, purpose limitation, storage limitation, and data security. An example of an Age-Appropriate design code can be found in the UK Age-Appropriate Design Code . For smaller and medium size enterprises, the Ministry of Post and Telecommunications can provide guidance and support in conducting self-assessments, should this be required.

2.4 Support awareness raising on online safety

Companies must support children, families and teachers in developing the digital skills required to stay safe online, as well as the socio-emotional and lifeskills that contribute to healthy decision-making and choices that may affect online safety and wellbeing. These initiatives 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. Recent evidence of what works in preventing online violence, including prevention education, can be found here. https://www.who.int/publications/i/item/9789240062061 These activities do not take away from the burden of responsibility that lies on companies to ensure that their products and services are safe and age-appropriate, and should not be used to imply that victims are to blame for not taking appropriate actions when they experience OCSEA and other forms of harm.

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.[7] 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,

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

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.

2.5 Creating a safe online environment

In addition to the adoption of safety and privacy by design principles and ensuring a child-rights-focused operating and delivery environment, digital technology companies in Cambodia can take additional steps to creating a safe online environment for children. These may include:

- The provision of parental controls. 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. Where companies provide or promote the use of parental control mechanisms, companies must make clear that these are less effective for older children, as children quickly gain the technical skills to circumvent them. Companies should also make clear that 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.

- Companies should always ensure that opt-out services are easily available and advertised, and that privacy settings (including location services) 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.

- 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.

- 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, as well as clear information on what data is being collected, the purpose of collection, and with whom it is shared. This should always be presented in a way that children can easily understand and follow, including children with disabilities.

2.6 Preventing and Responding to Child Sexual Abuse Material (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.

- 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.

- 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.

Reporting interfaces on websites or products may link directly to the reporting portals of authorized CSAM reporting Hotlines such as the IWF or NCMEC, if formal partnerships are in place. 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.

- Foster relationships with international agencies and partners, including those who hold or have access to CSAM image databases, such as the IWF and NCMEC, 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. 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.

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.

- 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. The use of any automated tools should always ensure that they are used in a way that does not undermine children's rights to privacy in any way,[8] and is consistent with the provisions, aims and objectives of the CRC, and respects the right to privacy of children.[9]

- 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. 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.10 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.

- 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.

[8] 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.

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

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

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 NCMEC) and a notification is automatically sent to the Cambodian law enforcement agency as well as the in-country INHOPE CSAM Hotline (currently operated by APLE) The law enforcement agency 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.

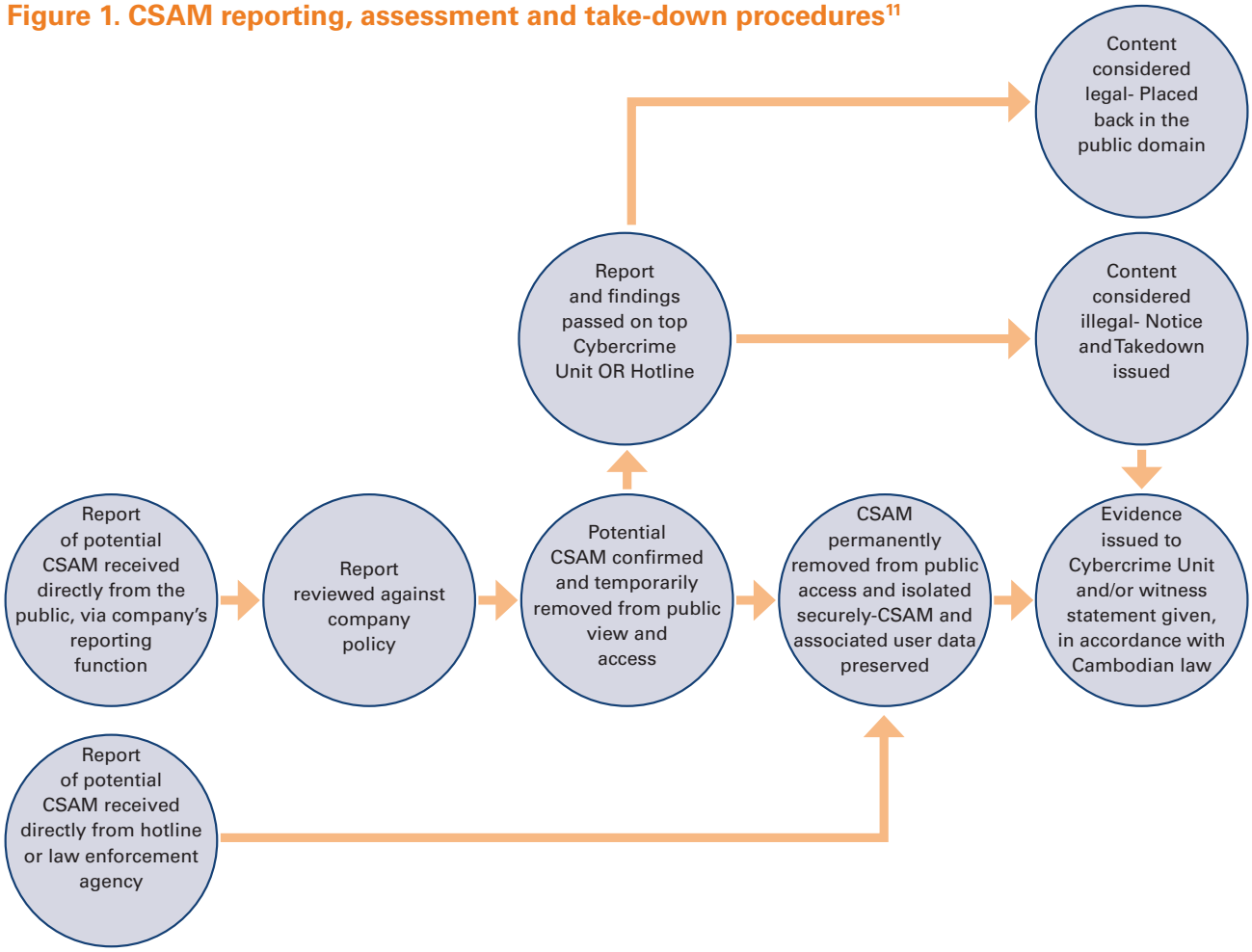
Any Takedown request (or Notice) originating in Cambodia, where CSAM has been identified in Cambodia, to an international social media or digital technology company, must come from the designated law enforcement agency, in Cambodia the Anti- Cybercrime Unit. Any CSAM reported through the INHOPE Hotline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

Notice and Takedowns can also be initiated by Cambodian law enforcement, usually based on information received from the public, or from a global digital technology company, NCMEC, 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.

- 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-Cybercrime Unit) (and may choose to also report to the CSAM Hotline), who will assess or refer for assessment of the content using a process similar to that detailed in Figure 1, 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.

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 Hotline and Cambodian Anti-Cybercrime Unit.

Figure 1. CSAM reporting, assessment and take-down procedures[11]



- 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.

  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).

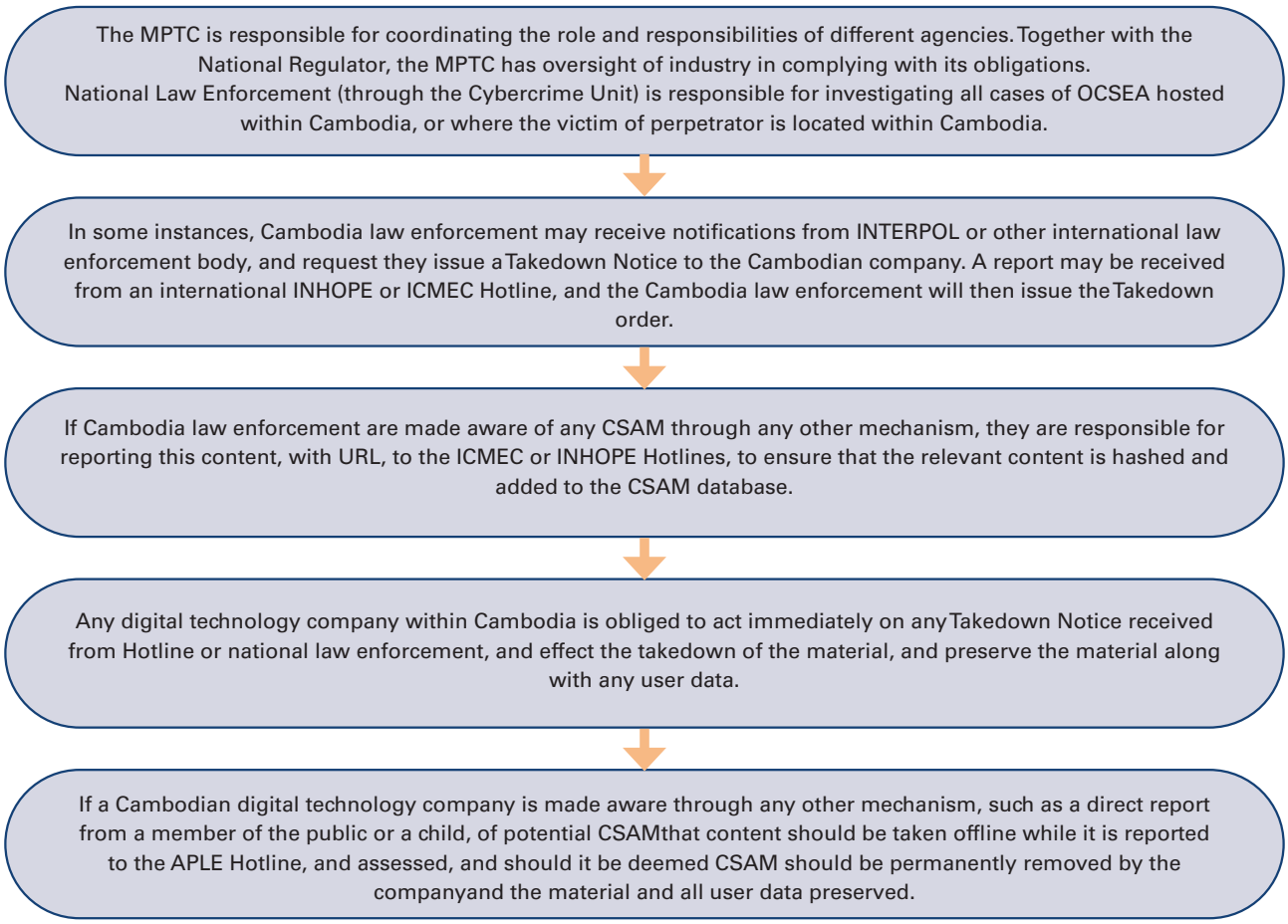
[11] UNICEF and GSMA, 2016, Notice and Takedown. Company policies and practices to remove online child sexual abuse material. Available online at https://www.gsma.com/mpoweryouth/resources/notice-and-takedown-company-policies-and-practices-to-remove-online-child-sexual-abuse-material/

- The evidence preservation procedures should also stipulate the process for the destruction of any illegal content following the mandatory retention period.

- 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.

As with the Child Rights Impact Assessments and self-assessments of privacy and safety by design, the MPTC may provide guidance and support to smaller companies in ensuring that the appropriate prevention and response mechanisms are established.

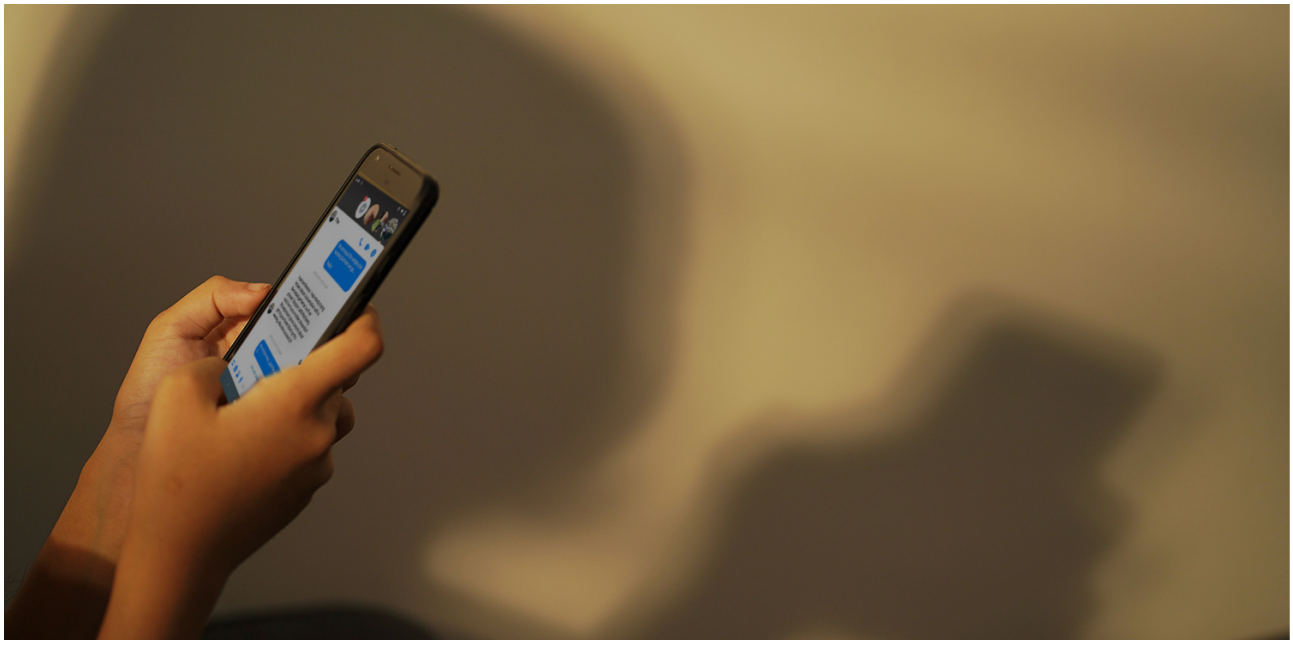


3. ASSESSING THE DIGITAL TECHNOLOGY INDUSTRY ACTIONS AND IMPACT

Ensuring that the safety, protection and wellbeing of children remain central to the provision of services and products requires more than a single, or single set of, interventions. All the actions outlined above should include mechanisms for monitoring the implementation process and the outcomes of each on identified child online protection indicators. These should be reassessed at regular intervals (between one and two years), to ensure that the desired impact is being achieved, and allowing for the early identification of any changes or improvements in companies own policies and processes impacted by child rights and online protection, and as well as on products and services that are brought to market.

This includes the provision of digital literacy, online safety and digital citizenship programmes, which should be assessed for any impact on knowledge translation and practice, rather than simply awareness.

Companies should also publish the results of these assessments in annual transparency reports. This yields the added benefit of ensuring that potential customers, and the public in general, are aware of the important steps that the digital technology companies are taking towards ensuring the products and services take into account the safety and wellbeing of children. An example of a self-assessment form for reporting in Cambodia is included in Appendix 2.



APPENDIX 1: 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.

APPENDIX 2:
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*	☐	☐	☐	☐

APPENDIX 3: 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)

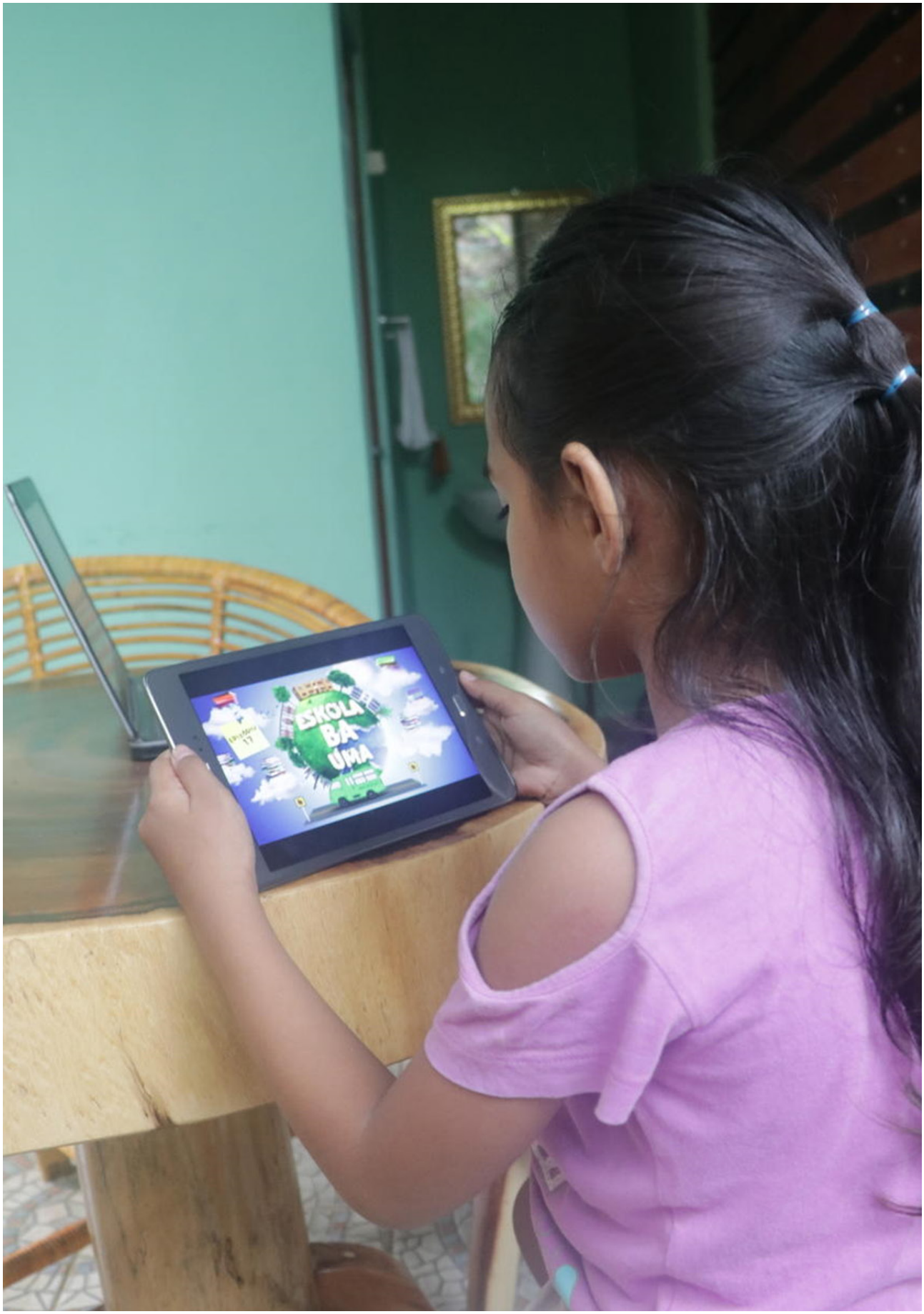
Software that allows users, typically a parent, to control some or all functions of a computer or other device that can connect to the internet. Typically, such programmes can limit access to particular types or classes of websites or online services. Some also provide scope for time management, e.g.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

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