GUIDANCE NOTE

WeProtect GLOBAL ALLIANCE

Implementing the **Global Strategic Response** to Eliminate Child Sexual Exploitation and Abuse Online

The **Global Strategic Response** framework is designed to help set objectives and provide a comprehensive global strategy to eliminate child sexual exploitation and abuse online. This document frames the response by thematic area, underpinned by cross-cutting approaches. The six themes are:

Policy/Legislation

Criminal justice

Victim support services and empowerment

Technology

Societal

Research and insight

WeProtect GLOBAL ALLIANCE

GLOBAL STRATEGIC RESPONSE: Eliminating Child Sexual Exploitation and Abuse Online

Theme	Policy/Legislation	Criminal justice	Victim support services and empowerment	Technology	Societal	Research and insight
Capabilities	**1 Political will** Accountable leadership & willingness to collaborate at the highest level. Adequate government resources dedicated to fighting the epidemic **2 Legislation** Comprehensive technology, including common definitions, terminology and thresholds to facilitate the harmonisation of criminal offences, obtain evidence, hold the private sector accountable and prevent unaccountable 'sovereignless' companies **3 International commitments** to capacity development (both cross-border technology-based improvements and systemic improvements within countries) and the prevention of ineffective state response systems	**4 Information sharing and collaborative targeting** Shared access to international databases: child sexual abuse material and offender targeting methodologies; formal data sharing frameworks; high value collective targeting **5 Risk/threat assessment matrix** for victim ID and offender targeting **6 Modernised reporting systems** reporting systems **7 Collaborative online expertise** Collaborative tech development to investigate offenders **8 Dedicated, trained officers and prosecutors** with expertise in tackling online child sexual exploitation and solutions for investigating encrypted content	**9 Crisis response** Effective and timely support **10 Victim and survivor voice groups** Advocates for change **11 Victim and survivor privacy and dignity** protected by the timely removal of all exploitative material **12 Victim identity protection** Preserve the anonymity of victims	**13 Innovative solutions** The use of technology, including artificial intelligence, to detect, block and prevent illegal and exploitive material, live streaming and online grooming **14 Technology-led risk and safety assessment** across platforms and upstream/ downstream providers **15 Voluntary principles for child safety, including safety by design** Wide and consistent adherence among tech sector **16 Increased transparency** Regularly publish transparency reports on detection & removal of child sexual abuse material, and ensure data are supported by explainable methodology	**17 Digital culture development** Demand for online child safely to be prioritised; built into and evolving the technology; increased public/citizen accountability of governments and companies **18 Informed media reporting** Ethical approach, consistent terminology **19 Restriction of children's exposure to illicit and harmful content online** Systemic restrictions to prevent child access to illicit content **20 Education and outreach** Regular messaging appropriate to age, gender and culture **21 Offender outreach** Develop targeted early interventions strategies	**22 Threat analysis and monitoring** Detailed and up-to-date assessments of threats and trends **23 Research to understand online vulnerabilities and effective safety education systems** Online safety and preventative approaches **24 Offender research** Offender behaviour, drivers, pathways and effective interdiction **25 Long-term victim trauma analysis** Mental health, societal and economic **26 Ethical AI and innovation** increased and sustained investments in ethical AI and safety-enhancing solutions
Outcomes	Renewal of high-level commitment at a national and international level Sufficient funding, focus and legal frameworks in place at a national level to prevent child sexual exploitation and abuse internationally	Resources are pooled to identify, pursue and apprehend offenders and rescue victims Successful joint investigations and prosecutions are conducted	Victims have access to the support they require	Industry, leverages and legislation to prevent their platforms being used as a tool for abuse Government and non-governmental organisations use technology and legislation to ensure platforms are not used as tools for abuse	Children are protected from sexual exploitation and abuse, no matter where they live. Parents are empowered to protect their children from online harm, no matter where they live. Public action holds government and companies accountable	Government, law enforcement, civil society, academia and industry have a clear understanding of the latest threats
	Formally renew WeProtect Global Alliance commitments Increase country members to the Alliance and strengthen engagement Criminalise child sexual abuse material consistent with Lanzarote Convention; develop common framework for content classification Prioritise the protection and privacy of children online in domestic and global policy Best practice legislation menu with regional samples Ensure laws and technology, including data retention, do not evolve in ways that increase online harms to children	Centralised online resource centre for all countries Investigative tools to counter anonymisation tech Consolidated image repository for Collective Victim ID analysis and targeting Formalise global investigative taskforce for collective high value targeting Formal data sharing frameworks, universal cooperation frameworks, and standards for legal interoperability	Standardised procedures for reporting images, material and contextual information to rescue victims Increase dedicated Child Advocacy Centres for all forms of child exploitation Standardised practices to protect the identity of victims Expand victims' voice groups	Regular reporting Strong law enforcement engagement and policies on legal compliance Proactive and responsive international engagement with technology sector Increase volume of technology sector prioritising child risk assessment and safety by design Broader use and application of Arachnid notice and takedown platform	Global public service announcement elevating priority of child protection in the digital world Further measures taken to reduce offending Children, carers, teachers and other responsible adults aware of risks and protection measures Awareness raised among the public Offenders and potential offenders can obtain services to prevent first-time offending and re-offending Understanding and countering increase in self-generated child sexual abuse material	Regularly updated insight into global trends and the impact of interventions, including through an annual Global Threat Assessment Deeper understanding of the long term impact of abuse, including the economic cost Deeper understanding of the impact of abuse into adulthood, including the economic cost Assessment of online safety education programmes
Partners	National governments, regional organisations, UN agencies and industry partners	National law enforcement, Interpol and regional partners	National and international civil society organisations with specialist expertise	International and national technology companies, industry associations, and national and international law enforcement	National governments, regional organisations, international and national civil society organisations	National governments, regional organisations, international and national civil industry, society organisations, national and international law enforcement, and academic institutions

Coordinated capacity building

Establish comprehensive model of capacity building that incorporates all sectors of Model National Response

Establish coordination between countries conducting bilateral capacity building

Dedicated training for policy leaders to develop the Model National Response

National and regional policy leaders trained to identify strengths, gaps and opportunities

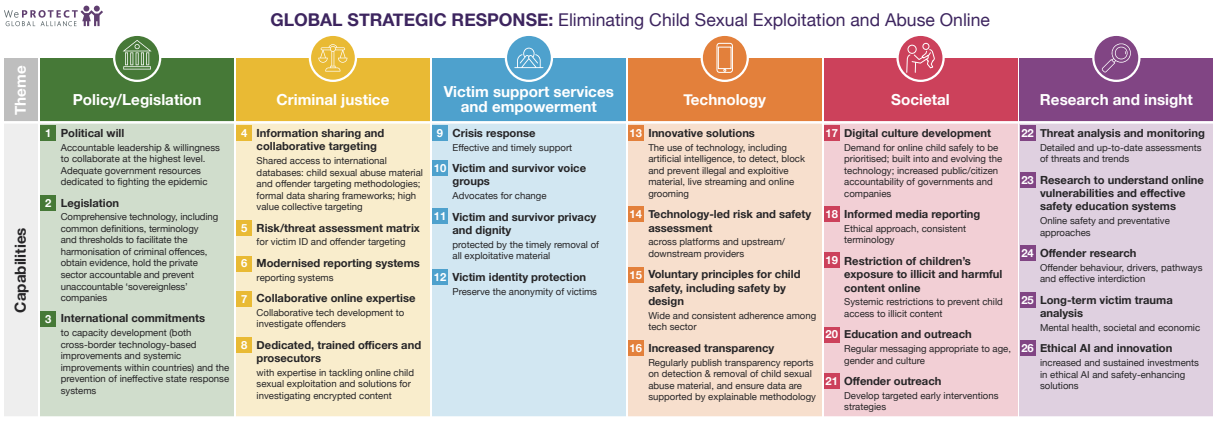
Acknowledgements

WeProtect Global Alliance wishes to thank its Board and membership for providing content, expertise and resources, and to Anna Gawn, Director of Stratagem International, for researching and compiling the Guidance Note.

Introduction

Overview and objectives

This guidance note aims to support practitioners and decision-makers across the globe to reach the outcomes outlined in the Alliance's Global Strategic Response (GSR) to eliminate child sexual exploitation and abuse (CSEA) online.



Specifically, this global guidance note was developed to support the practical implementation of the GSR. WeProtect Global Alliance (the Alliance) recognises the stark differences across countries and regions and places national and contextual specificities at the centre of any effective national response to CSEA online.[1] At the same time, however, it is necessary to acknowledge the universality and cross-border nature of CSEA online: there are no country borders on the world wide web. The GSR responds to this international dynamic and provides objectives and a comprehensive strategy for collaboration, coordination and shared learning to eliminate CSEA online at global, regional and regional levels.

This global guidance note aims to:

- **Build** on existing initiatives, programmes and experiences in addressing CSEA online;
- **Share** good practice and ways to overcome practical challenges for joint learning and collaboration, this includes experiences from the WeProtect Global Alliance's Model National Response (MNR);
- **Foster** global, regional and national collaboration between all stakeholders who have a role to play in eliminating CSEA online; and
- **Signpost** readers to relevant guidance, research and initiatives.

1 – For more information, please read: WeProtect Global Alliance (2016) Preventing and Tackling Child Sexual Abuse and Exploitation (CSEA): Model National Response, https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WeProtect+Global+Alliance+Model+National+Response+Guidance.pdf

Framing the Global Strategic Response

The GSR reflects the need for a coordinated multi-sector, multi-agency and multi-layered response to safeguard children both online and offline from child sexual exploitation and abuse. The GSR identifies six themes that are necessary to frame the response to CSEA online, in particular, and it details 26 capabilities which break down the themes into manageable areas for action. Intended outcomes for each theme are also detailed. A combination of themes and capabilities, or individual themes or capabilities, can frame specific programme initiatives. Agencies with expertise in one or more thematic areas will, naturally, focus on programmes or initiatives in those areas. At the same time, a wider perspective and comprehensive understanding of the situation should be maintained.

There are a number of cross-cutting themes that underpin all of the capabilities. These include:

- Establishing a comprehensive model of capacity building that incorporates all sectors of the Model National Response.
- Establishing coordination between countries conducting bilateral and regional capacity building.
- Dedicated training and professional development for policy leaders to develop the Model National Response, as well as a broad range of frontline workers to implement the MNR and GSR.
- Training for national and regional policy leaders to identify strengths, gaps and opportunities.
- Evidence generation and monitoring and evaluation to ensure evidence-based intervention and accountability.

The value of the GSR is its holistic overview; it recognises the mutual complementarity of the different themes and capabilities and reinforces the need to consider each theme and capability to effectively prevent CSEA online.

The GSR can also be used alongside other existing models and frameworks. Most relevant to mention here is *INSPIRE: Seven strategies for ending violence against children*, created by WHO, UNICEF and other international partners. INSPIRE is used across the globe to frame approaches to violence against children, it is relevant to online and physical abuse (especially as *"more often than not, those worlds blend into one"*). There are complementary overlaps between INSPIRE and the GSR that are useful to note when responding to CSEA online. That said, the GSR provides additional strategy areas that are necessary components for tackling CSEA online.

Intended Users

CSEA online manifests in a range of ways. It is assumed that readers of this guidance note have an existing basic understanding of CSEA online. An introduction to the associated crimes, with more detail and examples of cases can be found in the Alliance's *Global Threat Assessment*.

The guidance note aims to reach all practitioners and decision-makers across the globe who are involved in the elimination of online child sexual abuse and exploitation. Due to the necessary multi-sectoral, multi-agency and global nature of a strategy to prevent and respond to CSEA online, the intended primary users of the guidance note are wide-ranging. A broad list of intended users in national and international settings includes, but is not limited to:

- Policymakers, legislators, Parliamentarians, practitioners and related advocates;
- Criminal justice and law enforcement decision-makers, practitioners and lawyers;
- Organisations (governmental and non-governmental) working on child protection, this includes the social service workforce;
- Organisations (governmental and non-governmental) working on education provision;
- Civil Society organisations working with children;
- Media organisations;
- Technology companies/businesses and actors along their supply chains; and
- Academic institutions and think tanks working on online child sexual abuse and exploitation and evaluating research related to this field.

The participation of children throughout the design and delivery of programmes and services that affect them, including online programmes and services, is a principle of the UN Convention on the Rights of the Child (UNCRC) and is a common recommendation by experts engaged in this field of work. That said, children are not intended to be direct users of this guidance note; the focus is primarily on core practitioners and decision-makers. It is advised that these practitioners and decision-makers facilitate children's participation throughout their procedures and ensure their work in this field is informed by children's perspectives, including survivors/victims of sexual abuse and exploitation. Further information on child participation is provided in the relevant sections throughout the guidance note.

Who is the guidance note relevant for?

An effective response to CSEA online is multi-sector, multi-actor and international. It is important that **all** key actors and drivers of change are aware of the other components of the GSR framework and recognise the value and mutual complementarity of their contribution within a wider strategy. However, the skills, expertise and training of specific actors will be needed to lead and deliver certain themes of the strategy effectively.

Format and feedback

This guidance note has been informed by sector experts in governments, civil society, technology companies, law enforcement, academic institutions and intergovernmental organisations. The aim for this note is to sit alongside the framework on the WeProtect Global Alliance website.

The guidance note is a living document. In order to capture evolving practice, the Alliance will encourage its members to help review and update the guidance note regularly – as well as link to the GSR via their work. To share information, case studies and useful resources, please contact info@WeProtectga.org.

This guidance note provides the founding details for each capability and further reading is shared to give users more detail where required.

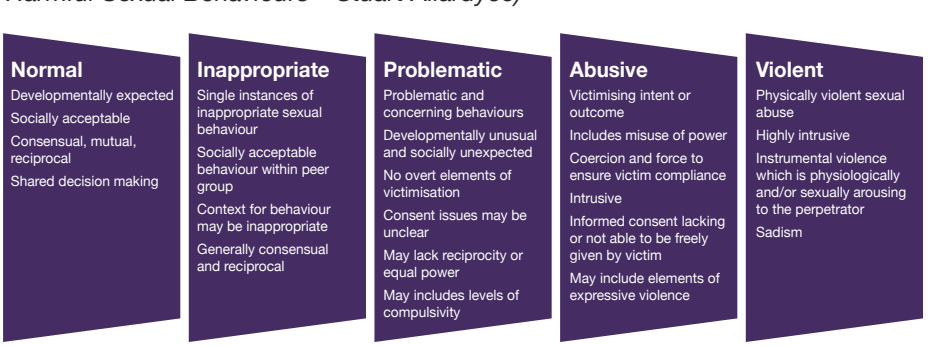
The format of the guidance note is based on the GSR. Each capability detailed in the GSR is broken down into five core areas:

- what it is;
- why it is important;
- relevance;
- how it can be implemented; and
- further resources.

Glossary and key definitions

Throughout this report we have adopted the following terms and abbreviations:

Term	Definition
Child Sexual Abuse	The involvement of a child (anyone under 18) in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or for which the child is not developmentally prepared and cannot give consent *(Source: WHO)*
Child Sexual Exploitation	A form of child sexual abuse that involves any actual or attempted abuse of position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another. *(Source: UN)* This can be perpetrated by individuals or groups of offenders.
Child Sexual Exploitation and Abuse Online OR Child Sexual Abuse Online	Child sexual [exploitation and] abuse that is partly or entirely facilitated by technology, i.e. the internet or other wireless communications. We use the term child sexual abuse and exploitation online, or 'internet enabled abuse', and not online child sexual abuse and exploitation to avoid characterising abuse online as distinct from abuse offline, since for victims the abuse is often not confined to the online realm.
Grooming children online for the purposes of sexual exploitation and abuse	Grooming is where an individual builds a relationship, trust and emotional connection with a child or young person in order to manipulate, exploit and abuse them *(Source: NSPCC).* Online grooming is when this process is facilitated, partly or entirely, by the internet or other wireless communications.
Livestreaming Child Sexual Abuse and Exploitation	Transmitting child sexual abuse and exploitation in real-time over the internet. Distant live streaming is a specific form of livestreamed child sexual abuse that is 'ordered' by an adult viewer and usually facilitated by another adult present with the child, either coercing or forcing them into conducting sexual acts *(Source: NetClean).* Livestreaming can also involve coercing a child to produce and transmit sexual material in real-time, see definition above.
Child Sexual Abuse Material	Any visual or audio depiction of sexually explicit conduct involving a person less than 18 years old (Source: NCMEC), whether real or not real.
Known Child Sexual Abuse Material	Child sexual abuse material that has been previously detected and classified by law enforcement and/or moderators.
First Generation Child Sexual Abuse Material	Child sexual abuse material that has not previously been detected and classified by law enforcement and/or moderators.
Child displaying harmful sexual behavior	A child or young person under the age of 18 years old exhibiting behaviours that are developmentally inappropriate, may be harmful towards themselves or others and/or be abusive towards another child, young person or adult *(Source: Harmful Sexual Behaviours – Stuart Allardyce)*



(Source: Continuum of children and young people's sexual behaviours - Simon Hackett)

GSR Theme: Policy / Legislation

Capability 1. Political Will

What is it?

- Senior level recognition that child sexual abuse and exploitation is a problem that leaders need to address, including where the internet plays a role (CSEA online).
- Allocation of government and company resources dedicated to eliminating CSEA.

Why is political will important?

- Indication of awareness of the issue, of harm it causes, of scale and need for actions at strategic political level and amongst key stakeholders.
- Greater likelihood of adequate legal frameworks, stronger policy, a robust law enforcement and judicial response, improved victim services - and a desire to hold online service providers to account.
- Commitment from political leaders and technology companies to plan, allocate resources (funding and people), and deliver actions that reach a set of objectives (e.g. in the MNR and GSR) aimed at eliminating CSEA online.
- It enables long-term planning and resource allocation commitments (e.g. throughout political cycles), which is crucial for sustainable change.

How can it be implemented?

- Nations can create a dedicated role, such as a national rapporteur or commissioner, to ensure continuing leadership and political will across changes in government.
- Build awareness and understanding of the UN Convention on the Rights of the Child (UNCRC), its Optional Protocol on the sale of children, child prostitution and child pornography and the forthcoming UN General Comment on children's rights in relation to the digital environment[2] (published in 2021).
- Demonstrate political leadership in acknowledging and shifting harmful sociocultural norms that perpetuate child sexual abuse and exploitation
- Build awareness and understanding of the risks, threats and opportunities for children of internet access and the role of governments and technology industry in developing a safe internet for children.
- Build understanding of the importance of international collaboration on all levels for an effective and strategic response.
- Build evidence and understanding of the implications that technology can have on children's cognitive, physical and socio-emotional development, on achievement of their full rights, and the associated medium- and long-term socio-economic implications.
- Recognise that "*the long-term effects of not investing enough in policies affecting children may have a profound impact on our societies*"[3].

2 – General Comments are highly authoritative and have a legal basis, they are automatically assumed and not ratified.

3 – European Commission (2012), European Strategy for a Better Internet for Children (EN version), *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0196&from=EN*

Further resources:

- Broadband Commission for Sustainable Development (2019) *Child Online Safety Report: Minimizing the Risk of Violence, Abuse and Exploitation Online*.
- Canadian Centre for Child Protection (2019), *How we are Failing Children: Changing the Paradigm*.
- End Violence Against Children Partnership (2019), *Ending Violence Against Children: Key messages and statistics* (full version).
- Livingstone, S and Haddon, L (2009) *Introduction: kids online: opportunities and risks for children*.
- WeProtect Global Alliance (2019), *Global Threat Assessment 2019: Working Together to end the sexual exploitation of children online*.
- UNICEF and ITU, GPEVAC, UNESCO, UNODC, WeProtect Global Alliance, WHO and World Childhood Foundation USA (2020), *Technical Note:* COVID-19 and its implications for protecting children online.
- WeProtect Global Alliance (2016) *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response*.
- Office of the e-Safety Commissioner legislative functions https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions
- UNICEF, *Review of the Evidence 2020, https://www.unicef-irc.org/publications/1183-investigating-risks-and-opportunities-for-children-in-a-digital-world.htm*

Capability 2. Legislation

What is it?

- A 'suite of legislation' that effectively defines and legislates against all forms of child abuse and exploitation, including on and offline offences, trafficking and slavery.
- Clear and consistent regulation to govern the detection and reporting of suspected CSEA online that removes any doubt or ambiguity over the deployment of targeted technical tools to assist in the identification and removal of child sexual exploitation material.
- Consistent terminology, including common definitions and thresholds to facilitate the harmonisation of criminal offences, obtain evidence, hold the private sector accountable.
- Legal confirmation that there are no spaces outside of the law: what is illegal offline should also be illegal online. Harmonisation of legislation should cover substantive and procedural law to provide harmonised standards in adjudicating and investigating cybercrimes.

Why is it important?

- Aligned national, regional and international legislation provides a common framework and sets norms for (global) citizens' conduct and behaviour online.
- Aligned national, regional and international legislation lays out the legal framework governing all actors (businesses, children, offenders, public), including responsibilities on reviewing, reporting, responding to and investigating reports.
- Aligned national, regional and international legislation and legal frameworks, including extra-territorial legislation, bilateral agreements and joint investigations. This provides responders with the basis for cross-border collaboration to prevent child sex offenders concentrating in countries with weaker legislation and procedures.

How can it be implemented?

- It is likely that a two-pronged approach will be necessary to ensure comprehensive cover: 1) Specific online or digital environment legislation will need to be developed or updated, and 2) key points relating to operating in a digital environment will need to be integrated into existing legislation.
- Comprehensive national, regional and international legislation should be grounded in the UNCRC and prioritise safe and empowering internet access for its youngest users.
- National, regional and international legislation should provide a clear set of online norms and behaviours, this includes regulations around reporting concerns or disclosures of abuse or offenders.
- National, regional and international legislation should ensure that technology businesses and other industry partners meet their child (and human) rights responsibilities and are held to account where there are causes for concern or cases of abuse are disclosed. Legislation needs to ensure that businesses can maintain growth, cooperation and innovation.

- Specific regulations must allow companies to proactively deter the upload of, identify and remove harmful images, videos, audio and text rapidly and on a large-scale from the internet.
- Opportunities should be sought to expand existing international law, e.g. The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, also known as "the Lanzarote Convention", to include more countries. Alternatively, new regional legislation should be developed in regions where no such conventions currently exist.
- Legislation should provide for effective deterrence of potential offenders as well as effective, rapid responses to reports of abuse (or suspicions of abuse) and investigations where necessary. This includes in cases where there is no evidence that contact sexual abuse has taken place.
- Special attention should be given to avoiding both intentional and unintentional criminalisation of victims and survivors of CSEA online.
- It is important to balance and maintain standards of security, safety and privacy. This includes the need for clear lines on identifiable data protection, consent (including for children and considerations for parents / caregivers) and rules of confidentiality need to be clarified. Safeguards should be in place to ensure there is transparency and accountability in the use of technological tools to identify and remove child sexual abuse material. In addition, detailed legislation should allow for access to particular identifiable data in cases where it is needed for a specific investigation purpose.

Further resources:

- African Union (2018) https://rm.coe.int/3148-afc2018-ws9-ocse-au/16808e85b9
- Child Dignity Alliance, Technical Working Group report
- Council of Europe (2020), *Information Note: The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (Lanzarote Convention).
- Council of Europe (2020), *Guidance note to respect, protect, and fulfil the rights of the child in the digital environment*.
- Council of Europe (2004), *Convention on Cybercrime* (Budapest Convention) European Union (2018), *General Data Protection Regulation*.
- International Centre for Missing and Exploited Children, *Child Sexual Abuse Material: Model Legislation & Global Review*.
- Internet Watch Foundation, *Laws and Assessment Levels webpage*.
- UK Government (2018), *Data Protection Act 2018*.
- UN Committee on the Rights of the Child, Guidelines on combating child sexual exploitation

Capability 3. International Commitments

What is it?

- International commitments to capacity development (both cross-border technology-based improvements and systemic improvements within countries) and to the prevention of inadequate or ineffective state response systems.
- In addition, this includes agreed processes for bilateral agreements and investigations.

Why is it important?

- International commitments set shared objectives to achieve over time in relation to eliminating online sexual abuse and exploitation. They are an initial step towards putting political will into practice and recognising the urgent need for a global, multi-sector, coordinated response to CSEA online.
- International commitments are generally made public and create national and global accountabilities for individual States and, in some cases, businesses. This enables national and international stakeholders to follow up on the commitments made. Follow up on implementing the commitment and measuring progress against pre-set indicators or milestones is critical (e.g. reflection of online rights abuses and opportunities in country child rights report to the Committee on the Rights of the Child).
- International commitments can allow for country, and business, comparisons, depending on the amount and quality of information shared. This can promote an aligned uptake of obligations and sharing of lessons and information on legislation, systems and good practice, particularly amongst countries within the same region or businesses in the same industry. It can also help avoid policy and regulatory fragmentation, which has the potential to undermine harmful online content.

How can it be implemented?

- By ratifying the UNCRC and the Optional Protocol on the sale of children, child prostitution and child pornography, States commit to upholding and protecting the rights and principles enshrined within both documents – this includes online as well as offline. The UN General Comment on children's rights in relation to the digital environment (published in 2021) will provide practical orientation for the implementation of child rights online. General Comments are highly authoritative and have a legal basis, they are automatically assumed and not ratified.
- By working under the UN Sustainable Development Goals 16.2 and 8.7 (among others), States and partners can ensure a consistent global response that ensures CSEA online is incorporated into the wider violence against children agenda.
- WeProtect Global Alliance's membership primarily includes governments, business and civil society. Each member commits publicly to working collaboratively with WeProtect Global Alliance and other members to eliminate CSEA online with the aim of ending it.
- WeProtect Global Alliance supports coordinated efforts with other bodies focused

on violence against children such as the Global Partnership to End Violence Against Children or online harms such as the International Telecommunications Union, the Internet Engineering Taskforce and the Internet Corporation for Assigned Names and Numbers so as to maximise collective impact and avoid siloes.

Further resources:

- Government commitments/statement of action for WeProtect Global Alliance.
- *Membership commitments / Partner Criteria* for the Fund to End Violence Against Children.
- *Membership Organisations* of the Child Protection Humanitarian Alliance.

GSR Theme: Criminal justice

Capability 4. Information sharing and collaborative targeting

What is it?

- Shared access to international databases, particularly those regarding child sexual abuse material and offender targeting methodologies; formal data sharing frameworks; high value collective targeting; and criminal records databases and other relevant criminal databases, e.g. ECRIS.

Why is it important?

- Efficient and effective online child protection and safeguarding strategies that respond to the needs of individuals and groups of children requires coordinated action across different actors, industries and countries.
- Due to the interrelated and international nature of CSEA online, programmes or strategies based on unaligned terminology, inaccurate data or mismatching definitions of risks are likely to be less efficient and effective, and create unnecessary obstacles in reaching a shared goal. Open collaboration from the outset will avoid unnecessary inefficiencies.
- Information sharing and collaborative targeting enables better decisions and facilitates more efficient prevention, early intervention and effective response.

How can it be implemented?

- Develop consensus amongst actors on the categories of children, offenders, technology gaps and other factors that will be used for data collection, technology design and reporting and response procedures. Include technical advice from child protection experts and other interested actors for aligned terminology.
- Develop information sharing and data protection protocols and referral pathways (signposting) for the immediate referral of children identified as victims, or potential victims, of online exploitation and abuse.
- Information sharing protocols should adhere to industry-wide ethics or principles and respect confidentiality. Key points include: (i) only collect personally identifiable data when the intended use is clearly defined, and (ii) only share information on a need-to-know basis and where there is consent (from the child as well as parent / caregiver where appropriate), or in cases where there is concern of potential harm for an individual or group of individuals. Capacity to consent should be considered as part of this process.
- Develop a set of shared indicators to outline progress towards effective collaboration and information sharing between *all* relevant actors.
- Establish baselines to understand trends over several months or years and only gather data that you will use.
- Identify potential risks (or unintended harm) that may be caused by data collection processes and mitigate against the risks. Before sharing information, consider the risks for children of sharing data that is unreliable, inaccurate, out of context or can be traced back to individuals.

- Ensure that all staff collecting, analysing and encrypting data have participated in training on data protection and understand the principle of confidentiality as well as the sensitive nature of the information that they are working with.[4] An additional standard should be that all staff should have training on impact of abuse on children and on child safeguarding in general.

Further resources:

- Sphere (2019), *The 2019 Minimum Standards for Child Protection in Humanitarian Action,* Pillar 1.
- GetSafeOnline (2018), *General Data Protection Regulation (GDPR).*
- Interpol website, *International Child Sexual Exploitation database*.
- University of New South Wales (2018), *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*.
- DLA Piper, *Database of data protection laws*

4 – Informed by / adapted from Sphere (2019), *The 2019 Minimum Standards for Child Protection in Humanitarian Action,* Pillar 1.

Capability 5. Risk / threat assessment matrix

What is it?

- Assessing risks for victim identification, offender targeting and to mitigate against technology infrastructure and broader online risks.

Why is it important?

- Children face a range of individual and combined risks[5], including those relating to sexual exploitation and abuse, when interacting in digital environments. The risks can manifest online and offline and come from a range of actors. Systematic and coordinated identification, assessment, management and mitigation of all risks is crucial to strengthening the safeguarding of children online and offline and to reducing the possibility of unintended (or intended) harms coming to life.
- Risk management is standard good practice in (offline) project management and operations. Therefore, all actors planning, delivering, supporting, strengthening and advocating to change a specific online or digital project should also identify and manage the associated risks.

5 – Risk is defined here as a chance or possibility that an individual will be harmed.

How can it be implemented?

- Technologies and behaviours can change and issues can emerge and change over time. To reflect the shifting environment, all actors should have a clear risk assessment template enabling them to assess, re-assess and add risks on a systematic basis. A thorough risk assessment process includes:
  - Defining and agreeing risks;
  - Identifying online and offline risks, including data and privacy-related risks;
  - Assessing the likelihood and severity of those risks (e.g. scale 1-5);
  - Identifying measures to avoid, eliminate, mitigate and manage risks;
  - Re-assessing the likelihood and severity of those risks with mitigation measure in place;
  - Documenting measures that are needed, associated responsibilities and timeframe; and
  - Reassessing risks at set timeframe.
- Risk assessments can be separated into broad areas/themes for analysis including: content risks; contact risks; conduct risks; and contract (or commercial) risks; excessive use risks and societal risks. Analysis should also cover perpetrator tactics/techniques, vulnerability scans, penetration testing and at-risk focus. Intersectional analysis is advised where possible and where not against confidentiality or privacy legislation.
- Input from stakeholders with varied expertise (e.g. technology engineers, criminal justice staff, and child protection professionals) across organisations, sectors and countries will strengthen the risk assessment quality.

Further resources:

- *A guide for tech companies considering supporting the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (2021)* WeProtect Global Alliance members ((*Facebook*, *Google*, *Microsoft*, *Roblox*, *Snap* and *Twitter*).
- 5Rights Foundation (2019), Towards an Internet Safety Strategy (see p5 for risk analysis).
- Girl Effect (2018), *Digital Safeguarding Tips and Guidance*.
- Information Commissioners Office (2018), *Consultation: GDPR DPIA Guidance*.
- Internet Watch Foundation (2018), *Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-Streamed Child Sexual Abuse*.
- SafeToNet Foundation, *App Risks*.
- Telecommunication Development Sector (ITU-D) (2020), *Child Online Protection Guidance note*, Separate documents available in different languages for children; parents; industry; and policy makers.
- WeProtect Global Alliance (2019), *Global Threat Assessment 2019: Working Together to end the sexual exploitation of children online*.
- Australian eSafety Commissioner, *Industry self-assessment tools*

Capability 6. Modernised reporting systems

What is it?

- A reporting system for CSEA online (also known as cybertip) promotes and enables the reporting of and response to images and videos of CSEA online to ensure an efficient criminal justice response. It also encourages reporting of suspicions and causes for complaint of CSEA online (e.g. where there is no hard evidence).
- Reporting mechanisms are set up so that users can report concerns. Once the reports are received, a filtering system (often using hashing or AI) is applied to remove abusive content.

Why is it important?

- Highly visible, accessible and child-friendly reporting systems can prevent and respond to online abuse. All individuals in society should be able to report any cause for concern, risk or disclosure of abuse that may cause harm to themselves or to others both online and offline, with dedicated categories of reporting for content that is suspected of being related to child sexual exploitation and abuse.
- Modernised cybertip can ensure that systems are in place to immediately respond to individual, or group, cases or issues, and to stop further associated harm.
- Modernised cybertip can increase the awareness of online harms amongst children, general users as well as potential offenders. It can also increase understanding of different online abuses and harms, thereby increasing the number of reports being shared.
- Modernised cybertip enables organisations to log, analyse and respond to concerns of harm and specific risk areas caused by or contributed to them.
- Having a modernised cybertip system in place demonstrates an organisation's commitment to safeguarding children online and to preventing and responding to online harms.
- Having a visible, accountable and effective reporting system in place with the accompanying filters (modernised cybertip) in place can increase awareness of how suspicions and reports are handled, thereby increasing trust and confidence in the particular tools, software or platform, and potentially (eventually) leading to a reduction in abusive use.

How can it be implemented?

- Reporting mechanisms - or links to reporting mechanisms - that are visible, accessible (including to children with disabilities) and age-appropriate (targeting the youngest potential user) should be put in place on every platform, tool and software. They should be streamlined and have reporting options that update with changes in technology and how people use the internet, including where possible an option to remain anonymous.

- Where possible and appropriate, the reporting mechanism back-end architecture and filter systems should be aligned (international, regional, country level as necessary) with the reporting mechanisms of other similar tools, platforms and software.
- Aligning reporting mechanism and response procedure architecture internationally, regionally and/or per country will allow for effective, coordinated response and criminal justice procedures. It can better enable trend monitoring and analysis, avoid duplication of efforts, and avoid personally identifiable reports being sent unnecessarily to a number of organisations.
- To encourage user reporting, age-appropriate education and empowerment is required on: (i) what exploitation and abuse is, (ii) the associated risks, (iii) how to report, and (iv) what happens when a report is made. (See capability 9).
- Ensure appropriate acknowledgement of every report to foster trust in the system. Appropriate acknowledgement could include anything from a generic email to a personalised response.
- Where possible, all tools, services or platforms should install filters to prevent real-time activity that can lead to inadvertent or conscious child sexual exploitation and abuse. Preferably, this should be done at the design stage. E.g. Filters can prevent users from visiting foreign websites that contain images of children being sexually abused.
- Where reports have been received and abusive content or risks of abuse verified, businesses should commit to redesigning and adapting tools, services or platforms to respond to the abuse and / or mitigate the risks identified, e.g. gaming terms, enforced protections not enforced, immersive and addictive technology, incomplete filters and inaccurate or inaccessible signposting.
- An independent grievance redressal mechanism for victims/complainants is needed to address instances where CSAM is reported but not taken down despite court orders (per the Indian guidelines). Intermediaries need to be held accountable, especially for legal obligations, beyond the regularly published reports.

Further resources:

- Council of Europe (2019), *Mechanisms for collective action to prevent and combat CSEA online*.
- Cybertip.ca, *Report Form* (webpage).
- Internet Watch Foundation, *International Reporting Portals* (webpage).
- Project Arachnid, *Project Arachnid website*.
- The US Government, *CyberTipline Modernization Act of 2018*.

Capability 7. Collaborative online expertise

What is it?

- Collaborative technology development to identify and investigate offenders.

Why is it important?

- Good practice experience from multi-country programme delivery (online and offline) consistently reinforces the shared learning, improved efficiency and effectiveness, and quality outputs that can result from collaboration across organisations, industries and countries.
- The Lanzarote and Budapest[6] Conventions mandate country cooperation when responding to CSEA online. This includes a shared legal basis for criminal cooperation when dealing with: victims and offenders based in different countries, individuals who are living in countries where they are not citizens, situations where extradition may be necessary and in other relevant criminal matters (Lanzarote Convention).
- The industry actors that focus on eliminating CSEA online is relatively small but growing. Collaboration is key to achieving agreed targets: a lack of efficiency and effectiveness can have significant implications on individual and groups of children.

How can it be implemented?

- Develop joint multi-country legislation, or national legislation based on international commitments and standards (see capabilities 2 and 3). This could include expanding the countries who have committed to the Lanzarote and Budapest conventions.
- Identify one 'model' (based on existing practice and systems) to guide international, or regional, criminal justice collaboration architecture and practice. Adapt and update the model collaboratively based on practice, need and over time.
- Define, agree and share case priority / urgency levels (based on harm or potential harm to a child), with practical examples, and assign appropriate follow up action, responses and responsibilities.
- Complete and share detailed criminal justice stakeholder analysis which details the roles, responsibilities and contributions of individual actors or stages within the wider CSEA online industry and architecture.
- Foster industry-wide support from all relevant stakeholders, including businesses, and engage their active participation in joint criminal justice policies, systems and practice. Reinforce the necessary combination of individual quality plus mutual complementarity to reach goals.
- Avoid intra-industry or intra-country competition and duplication of resources on the elimination of CSEA online. This could be achieved in part by creating open source tools and / or tools that are free at the point of use.

6 – The Convention on Cybercrime of the Council of Europe

- Develop and carry out joint training, research, risk monitoring and analysis, and evaluations of intervention programmes and other practical experiences.
- Ensure shared terminology and / or develop aligned systems to record, store, manage and share victim and offenders' data. Agree procedures through which personal data is shared on a need to know basis and in order to facilitate criminal proceedings.

Further resources:

- Commonwealth Cybercrime Initiative (CCI)
- Council of Europe (2019), *Mechanisms for collective action to prevent and combat CSEA online: A comparative review*.
- Cyber Security Programme of the Commonwealth Telecommunications Organisation (CTO), *Commonwealth Cybergovernance Model* and *General Cybercrime response*.
- ECPAT (2016), *Terminology Guidance note for the protection of children from sexual exploitation and abuse*.
- Internet Governance Forum (IGF), *Dynamic Coalition on Child Online Protection*.
- Interpol, *Cybercrime*.
- Global Partnership to End Violence against Children, *Safe Online*.
- UN International Telecommunications Union (ITU), *Child Online Protection*.
- WeProtect, *Commitments*.

Capability 8. Dedicated, trained officers and prosecutors

What is it?

- Ensuring that dedicated law enforcement officers, prosecutors and the judiciary have an expertise in tackling CSEA online and developing solutions for investigating content.

Why is it important?

- Officers and prosecutors, generally, have a strong understanding, experience or expertise in the technical area that they are investigating. Dedicated resourcing to tackling child sexual exploitation and abuse, including dedicated training around the online aspects and offences, should ensure a relevant, accurate and quality criminal investigation, response and solution.
- Cybercrime methods are constantly developing and, to be effective, officers and prosecutors need to remain in line with or ahead of developments. This includes maintaining a detailed understanding of encrypted content as well as cybercrime collaboration, methods, tools, platforms and software.
- It is important for all involved to have a victim-focused approach and understanding of the impact of crime on victims, as well as of offender behaviour.

How can it be implemented?

- Develop, or identify and adapt existing, training and professional development for all actors in the criminal justice system and child protection systems who will work on tackling CSEA online, including civil society and victim support services.
- Training and capacity building should be contextualised and utilise local knowledge, where possible.
- Systematic monitoring and analysis of the cybercrime environment and its changes is necessary to ensure that training, mentoring and coaching remains relevant. This should include offender methodology and the tools, platforms and software they use.
- Ensure that officers and prosecutors have access to shared case priority / urgency levels and are aware of their responsibilities and the appropriate follow up and responses (see competency 7).
- Ensure that officers and prosecutors have access to other individuals, including from other countries, who work on the same topics for shared learning and peer support.
- In addition to initial training, officers and prosecutors' expertise needs support to develop, grow and remain relevant. This can include but is not limited to: refresher training, coaching opportunities, mentoring advice, sharing relevant news and analysis, and attending relevant (regional or global) conferences, including virtual conferences.
- Ensure that officers and prosecutors, and their employers, can receive appropriate training and support so that they can maintain their own self-care, protection and wellbeing and manage the information on CSEA online that they see so as to avoid secondary trauma.

Further resources:

- The British Psychological Society (2020), *Taking trauma related work home – advice for reducing the likelihood of secondary trauma*.
- Interpol, *Global Learning Centre*.
- Lucy Faithfull Foundation, *Expert Child Sexual Abuse and Exploitation Training*.

GSR Theme: Victim support services and empowerment

Capability 9. Crisis response

What is it?

- To support and protect children, relevant, timely and individualised child-centred, multi-sectoral crisis response services should be provided to all child victims of sexual exploitation and abuse (and their families).
- Child protection crisis response and longer-term services include a range of coordinated services that may be provided online and / or offline:
  - safety and security services (e.g. physical removal from a location / abuser or removal of an offender from a particular site);
  - health services (e.g. physical and mental health and psychosocial support services);
  - justice services (e.g. prosecution and law enforcement of offenders); and
  - child and social welfare services (e.g. protection and care, including alternative care).
- Education and empowerment programmes and services for individuals and groups of children, their parents and caregivers and the wider society are also provided.
- Referral to other sector services may also be necessary (e.g. nutrition, asylum, disability, social protection).

Why is it important?

- Every child has a right to protection from exploitation or abuse in the first instance. For those that have been abused, a child protection response is required in the short and longer term, until a long-lasting solution has been reached. Duty-bearers[7] have a responsibility to protect children and to respond to reports or risks of exploitation and abuse accordingly, this includes providing protection crisis response services to children, their families and others as required, when a child is at risk of being or has been harmed or abused.
- Crisis response is crucial to prevent further harm or harm from happening in the first place. Longer term services are required so that the child can receive the services and support needed to rebuild their lives over time and to survive and thrive.
- Children's rights and duty bearer's responsibilities must be respected online as they are offline.
- Duty bearers have an ethical responsibility to educate and empower children to understand the online world and to foster safe and empowering online experiences for all children and general users.
- Effective crisis response, combined with the procedures and actions listed in capabilities 10, 11 and 12, can help give child victims and survivors more confidence, control and power over important choices within their lives.

7 – Duty bearers include the State / government as well as non-state responsibility-holders, including civil society, businesses, parents and caregivers. Duty bearers have duties and obligations under the UNCRC; they are legally bound to respect, protect and fulfil children's rights.

How can it be implemented?

- Multi-agency support for children's protection should align with the child protection system of the country in which the child victim is based. Child protection services should also consider that children are part of an interconnected online and offline "ecological system" and reflect the needs, rights and responsibilities of the individual, family (or care setting), community, and wider society.
- Ensure that one qualified individual is responsible for managing each case and ensures appropriate follow up, support and referrals throughout the process.
- Ensure that report responders (cybercrime officers and prosecutors, health professionals, other qualified individuals) are able to assess the priority of a case and follow up as appropriate (see capability 7 and 8).
- Empowerment and education services should reflect a balanced understanding of the threats, risks and opportunities for children.
- Age-appropriate, concise and accessible education is required for children, parents and caregivers and general users on: (i) what child exploitation and abuse is, including CSEA online (ii) the associated risks, (iii) how to report it, (iv) what happens when a report is made, and (v) different individual's roles and responsibilities in keeping children safe from sexual abuse and exploitation and generating a safe and empowering internet for all.
- Education and empowerment services can include signposting to reporting mechanisms, educational advertisement and further information on every platform, tool and service.
- Empower children, parents and caregivers and general internet users to prevent abuse and report suspected abuse. Some suggestions to achieve this include informing users about how reports are responded to and by whom, confirmation that reports can be anonymous, how reporting can help keep others from (further) harm, and the risks of not reporting. Also, success stories of responses to other reports can be shared to foster trust in the system.
- Ensure appropriate acknowledgement of every report, this can help foster trust in the system. Appropriate acknowledgement could include anything from a generic email to personalised response.
- Where high priority cases and / or cases that require specific support (in-person or virtual) are received, individualised follow up and intersectional analysis8 of the case by a qualified professional is required to inform the necessary services. Qualified professionals should have access to an up-to-date "referral pathway" so as to enable quick referrals to locally available, appropriate and accessible services.

Further resources:

- Canadian Centre for Child Protection, *Programmes and Initiatives webpage*.
- NSPCC (The UK Children's Charity), *Our Services*.
- Contextual Safeguarding approach, *https://contextualsafeguarding.org.uk/* The Global Protection Online Network *https://www.mariecollinsfoundation.org.uk/gpn*
- UNICEF, *2020 Evidence Review*

8 – Intersectional analysis will consider culture, race, gender, class, language and other factors as relevant, and assign an appropriate response.

Capability 10. Victim and survivor voice groups

What is it?

- Victims and survivors are a vital part of understanding the impact and best responses to CSEA online. With their consent and supported active participation throughout, it can be possible for them to advocate for change, including behaviour change, systems change and technology infrastructure change.
- With informed consent, it may be possible to work with victims and survivors to share their stories and/or advocate for change, as well as design programming and support services, campaigns and strategy.

Why is it important?

- Victims and survivors have the most authentic understanding and experience of child sexual abuse. This experience is important to inform responses, raise awareness and shape policy.
- Victims and survivors can shape and design responses and services as leaders with lived experiences.
- Victim and survivor groups can bring together children / young adults with similar experiences of online sexual abuse and provide a safe space for them to share challenges, fears and opportunities, build relationships with others who have similar experiences. It can be an important part of the recovery pathway.
- Victim and survivor voice groups can be a (supervised and safe) forum for peer-to-peer psychological first aid and mental health support for child sexual abuse.
- Victim and survivor groups, combined with the procedures and actions listed in capabilities 9, 11 and 12, can help give child victims and survivors more confidence, control and power over important choices within their lives.

How can it be implemented?

- Provide opportunities (including anonymously initially if required) for child victims to share or report their experiences of online sexual abuse. This must be accompanied by a process of rolling and informed consent based on age-appropriate and accessible language.
- Provide a personalised response by a qualified professional to acknowledge the report and respond accordingly. Initial response should ensure that the child is no longer in immediate harm and that any necessary crisis response services have been provided. (See capability 9).
- Create a forum location (online or offline) and share details with children on why they may want to engage with peers who have had similar experiences, how to engage, and who they will engage with (one adult with professional psychosocial qualifications should always be present).
- Set rules for the discussions and advise a focus on safe discussions, mutual respect, listening and engendering a supportive environment.

- Work with consenting children to develop anonymous stories that can be shared publicly. Engage communications and advocacy specialists to share the stories in different ways, through various media to target different audiences, where in the best interests of the child to do so.

Further resources:

- Canadian Centre for Child Protection, *Phoenix 11*.
- Canadian Centre for Child Protection, *International Survivors Survey*.
- ECPAT International (2019), *Guidelines for Ethical Research on Sexual Exploitation involving Children*.
- Marie Collins Foundation, *Meeting the needs of children abused online*
- UNICEF, *Ethical Research for Children*, Reporting for Children

Capability 11. Victim / survivor privacy and dignity

What is it?

- The protection of the victims' privacy and dignity by the timely removal of all exploitative material.

Why is it important?

- Removing exploitative and abusive material is critical for victims of CSEA online. It can also avoid any further re-traumatisation for the victim caused by re-sharing the abusive material.
- Understanding that the material has been removed may be an important step for an individual victim's emotional recovery, dignity and future mental health.
- The removal of harmful material, combined with the procedures and actions listed in capabilities 9, 10 and 12, can help give child victims and survivors more confidence, control and power over important choices within their lives.

How can it be implemented?

- Effective coordination across all relevant stakeholders (including civil society, law enforcement, child protection services, business and government regulators) will ensure an effective and non-duplicative response and provision of victim support.
- A pre-agreed understanding (e.g. a response plan) should outline (i) who is responsible for identifying and removing the abusive material from certain locations or sites, and (ii) how this is done (i.e. via reporting platforms, police and tech companies). National, regional and international considerations, as well as capacity, responsibility, resources, access and language are key considerations for when agreeing a response plan. When developing plans, focus should remain on the most effective response for the child.

- The continued development and wider application of hashes, AI, filters and other content removal tools is important for delivering faster and more accurate identification and removal of exploitative material.
- Further training across organisations, countries and continents on the removal of abusive material will increase the capacity and availability of individuals qualified to respond in an appropriate and qualified manner.
- Any communication with victims on this matter must be done by a qualified professional and in line with data protection regulations and agreed victim communications standard operating procedures.

Further resources:

- IWF: Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System (Dr. Weixiao Wei *https://www.iwf.org.uk/sites/default/files/inline-files/IWF%20Research%20Report_%20Development%20of%20an%20international%20internet%20notice%20and%20takedown%20syste_1.pdf*

Capability 12. Victim identity protection

What is it?

- Preserve the anonymity of child victims.

Why is it important?

- "*Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*"[9].
- The re-traumatisation of abuse or exacerbation of trauma for victims, due to child sexual abuse material (CSAM) still being available on the internet, is one core challenge associated with CSEA online.
- Also, the publication of personal information of a child victim can add more dimensions to recovery, dissuade future disclosures or reports of concern and hamper cooperation with authorities and social service professionals.
- Victim identity protection, combined with the procedures and actions listed in capabilities 9, 10 and 11, can help give child victims and survivors more confidence, control and power over important choices within their lives.

9 – European Union (2016), *General Data Protection Regulation (GDPR)*, Recital 38. The data requested must be necessary for the delivery of the service or application in question.

How can it be implemented?[10]

- All actors need to respect children's rights to privacy and the protection of personal data in the context of the internet and digital technologies.
- Businesses and other actors must gather children's personal data on the principle of "data minimization" or a "need to know" basis only.[11]
- Relevant data should be gathered and in a manner that is legitimate, well informed / understood, free, fair and consented (by parents or guardians and / or children, as per local legislation).
- Requesting consent gives children control over how their personal information is used and shared, and empowers children to understand and exercise their right to privacy.
- Age verification techniques can be put in place to ensure that consent and other protocols are in place.
- No website, platform, product, service or application should share children's personal data publicly by default. Children must be empowered to protect their privacy and adjust their privacy settings based on an informed understanding of opportunities and risks.
- No game or application should automatically activate a webcam. Information should be shared and consent received (from child and/ or parent or guardian) before a webcam is switched on.

Further resources:

- UNICEF (2018), *Industry Toolkit: Children's online privacy and freedom of expression*.
- UNICEF, *Children's Rights and Business in a Digital World, Discussion Paper Series: Privacy, Protection of Personal Information and Reputation Rights*.

10 – Informed by: UNICEF (2018), *Industry Toolkit: Children's online privacy and freedom of expression*.

11 – European Union (2016), General Data Protection Regulation (GDPR), Article 6 (1)(c).

GSR Theme: Technology

Capability 13. Innovative Solutions

What is it?

- The use of technology, such as artificial intelligence (AI) and machine learning, to prevent, detect, block, report and remove illegal and exploitative material, live streaming and grooming. It can also be used to deter and detect offenders and identify victims.

Why is it important?

- Due to the prevalence of existing CSAM online, and the likely extent of undetected CSAM on the dark web, technology (including real time image and video production, image and video distribution, image and video storage) needs to make rapid and extensive progress to identify and remove the existing levels of CSAM online as well as to prevent new cases and respond to active cases.[12]
- Methods to access different children and to commit CSEA online – both in terms of viewing CSAM but also grooming victims for CSEA - are ever changing and evolving. Offenders are likely to collaborate and share methodologies and tactics to bypass safety mechanisms and to share vulnerable profiles or existing abusive content.
- Similarly, on some sites, profile types can be recommended to those who have shown a prior interest in children – in some cases this will be recommending children to adults.[13]
- Technology can be used to deter offenders through targeted messaging, messages when questionable behaviour is identified and signposting to sources of help to address offenders/potential offenders' behaviour. This can help to create an internet where offenders feel less safe, more inclined not to take risks – and can easily seek help to change.

How can it be implemented?

- Carry out research and identify innovative practice to "*build crucial technological tools needed to more effectively prevent and work to eradicate child online sexual exploitation and abuse*".[14]
- Monitor effectiveness of interventions and share as a public good.
- Build on or expand the existing *Voluntary Principles to Counter CSEA online* to reinforce a set of basic industry standards to be met by all providers.
- Access and utilise existing principles, frameworks and assessment tools that have been developed to ensure safety considerations are embedded into the design, development and deployment of online products and services, like Safety by Design.

12 – End Violence Against Children, *Safe Online*.

13 – 5Rights Foundation, *Risk-by-Design microsite*.

14 – Technology Coalition, *Project Protect*.

- Removal of the harmful content as soon as it is identified should be considered on the grounds that it is likely that the risks and potential harm of keeping the content online are higher than the potential costs, or inconveniences, of unintentionally removing non harmful material. Once the material has been analysed, or re-reviewed (by a person or AI), it can be returned online if deemed unharmful.
- The allocation of dedicated resources and staffing with relevant training to tackle CSEA online.
- Collaboration and sharing of tools between technology firms, civil society and governments.
- Provide internet users with details of how to report illegal material with specific categories for that relating to CSAM and CSEA.
- When appropriate and where available, information on interventions for those who are at risk of offending (for example, providing links to support services) is also critical.

Further resources:

- 5 Country Ministerial, *Voluntary Principles to Counter CSEA online*.
- Technology Coalition, *Project Protect*.
- Thorn, *Safer*.
- *A guide for tech companies considering supporting the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*, (Facebook, Google, Microsoft, Roblox, Snap and Twitter).
- The Lucy Faithfull Foundation/Stop It Now! UK and Ireland, *online deterrence/EVAC funded IWF/LFF chatbot.*
- Australian eSafety Commissioner, *Safety by Design*
- Child Dignity Alliance, Technical Working Group
- UNICEF, *Encryption, privacy and children's right to protection*

Capability 14. Technology-led risk and safety assessment

What is it?

- Risk and safety assessment across platforms and upstream / downstream providers, in terms of both the risk to children but also for offender management.

Why is it important?

- A series of design decisions inform the development of a digital service or product. It is likely that these decisions are largely based on ensuring the wide promotion and use of the service or product in question. The extent to which design procedures assess and act on the risks and potential harm for children is unknown.[15]

15 – In the UK the Age appropriate design code will become law on 2 September, 2020: Information Commissioners Office (UK) (2020), Age-appropriate design: a code of practice for online services.

- A preventative and proactive approach to ensuring that user safety is embedded into the design, development and deployment of online and digital products and services is required - Safety by Design. A Safety by Design approach necessitates the need for ongoing considerations of age-appropriate design and access to services, in line with the end-user's maturity and evolving capacities
- Childhood has various cognitive stages and, subsequently, inherent vulnerabilities. This unregulated approach to design can create situations where children are engaging with subtle and 'persuasive technology'[16] without the requisite understanding, awareness and maturity to manage any risks or harm that they may face. For example, without their or their parent's knowledge children can be pushed towards increased engagement (including with individuals they do not know and adults) and lower privacy. Recommendation algorithms determine the content children see and/or the new 'friend' profiles that are suggested to them. Also, profiles are often set as public by default which can predetermine the visibility of children's identity and interests without their knowledge, understanding or consent (from them or their parents).
- Children may be put at risk by pursuing public 'likes' or sharing content. Examples include liking or sharing abusive or bullying material (which could be deemed as a public endorsement) and exchanging sexual acts or imagery. In addition, in some circumstances, 'commercial pressures' from advertising or gaming platforms on children can be used as a grooming tool by offenders wishing to exploit children's desire to compete in games and/or access 'lootboxes', game bonuses etc.
- This needs to be balanced with the need to empower and provide children and young people with controls and tools to manage their own experiences.
- Moreover, without visible channels for reporting abuse or causes for concern and accompanying information on every digital service or product, children (and adults) don't know how, why and what to report. This raises the likelihood of a 'cyberbystander effect' and limited reporting.
- As one billion children use the internet, the potential risks associated with subtle, seemingly small and unnoticeable design features are maximised.[17]
- Additional approaches are required to deter offending, too. Key principles of situational crime prevention are:
  - Reduce opportunity
  - Increase risks (of getting caught)
  - Reduce rewards
  - Reduce provocations

16 – The technology designed with the underlying motive of modifying a certain attitude of behavior, exploiting psychological and sociological theories, such as persuasion and social influence.

17 – Informed by: 5Rights Foundation, *Risk-by-Design microsite*.

How can it be implemented?

- All digital services or products should carry out child risk and impact assessments and safety review processes in the design phase (or retrospectively), and systematically thereafter, to understand the potential risks, and resulting implications, for children – as well as in terms of managing and mitigating potential offending behaviour.
- Risk assessments should consider a range of setting and use scenarios, assess how various design features interact when in use at the same time, and identify any potential resulting risks. Specific considerations in assessing scenarios and particular features could include: i) comparative assessment of the risks of public likes and whether a private 'like' feature reduces risks and simultaneously provides the required engagement with services and products, and ii) comparative assessment of the risks in scenarios where all children (all individuals up to the age of 18) are given safe and privacy-preserving settings by default.
- Vulnerability assessments can also be carried out to understand the vulnerabilities of different groups of children to online sexual abuse and exploitation. For example, factors to consider include socio-economic status, location, age, education level, disability, and family status (e.g. in alternative care).
- Child risk assessments and vulnerability assessments should aim to reflect children in both specific groups and a collective manner, they should also reflect the differences between children and intersectional analysis (e.g. gender, age, location, language, ethnicity etc.). All assessments should include children's own voices and perspectives.
- A collective set of minimum approved risk levels should be made transparent and agreed to by core actors and changes based on the child risk assessment findings should be made where necessary.
- Ideally, a standard basic format for child risk assessments should be developed and shared amongst actors to support those who do not have the capacity or resources and to promote an industry-wide basic minimum child risk assessment framework (or key contents).

Further resources:

- eSafety Commissioner (Australia), global *Safety by Design* initiative.
- Lucy Faithfull Foundation, *Services*.
- Lucy Faithfull Foundation, Preventing child sexual abuse.
- 5Rights Foundation, *Risk-by-Design microsite*.
- UNICEF, Recommendations for online gaming industry

Capability 15. Voluntary principles for child safety, including safety by design

What is it?

- Wide and consistent adherence within the technology sector of principles, and subsequent action, for child safety.

Why is it important?

- Keeping children safe from online sexual exploitation and abuse requires systematic cross sector collaboration and action based on widely agreed and shared principles. A broad range of principles can provide a framework that is relevant to all actors for collective action on eliminating CSEA online.
- The technology industry has a duty of care to consider children's rights and safety at the design phase and throughout the product lifecycle to ensure that reasonable and age-appropriate safety features (prioritising the youngest potential user) are built into all digital products and services.

How can it be implemented?

- Identify an industry-wide set of principles that are relevant and applicable to all actors engaged in reaching the goal of eliminating CSEA online, e.g. 5 Country Ministerial, *Voluntary Principles to Counter CSEA online*.
- Agree as a core minimum that the best interests and dignity of all users should be considered in the design and use of products and services - with Safety by Design a core business objective. .
- Three principles are highlighted in the Australian eSafety Commissioner's Safety by Design initiative:
  i. **Service provider responsibilities:** the burden of safety should never fall solely upon the end user. Service providers can take preventative steps to ensure that their service is less likely to facilitate, inflame or encourage illegal and inappropriate behaviours;
  ii. **User empowerment and autonomy:** the dignity of users is of central importance, with users' best interests a primary consideration.
  iii. Transparency and accountability: Transparency and provide assurances that services are operating according to their published safety objectives, but also assist in educating and empowering users about steps they can take to address safety concerns.
- Ensure understanding and buy-in from all actors, including business, children and parents, on the principles. Fostering ownership and building understanding of the principles across actors can be crucial to their ultimate use.
- Communicate the principles to different actors through various forms of media to foster interest and uptake. Aim to create a system whereby all actors across the industry, including business, children and parents, feel motivated to publicly endorse and commit to the shared principles.

- Set indicators, standards and create tools to measure uptake and actions towards reaching the principles over time. Regular monitoring, reporting and review on implementation and progress can be done collaboratively and/or independently. The process should be transparent and shared publicly; sharing efforts and progress could support others in initiating and strengthening their efforts.

Further resources:

- eSafety Commissioner (Australia), global *Safety by Design* initiative.
- Information Commissioners Office (UK) (2020), *Age-appropriate design: a code of practice for online services*.
- 5 Country Ministerial, *Voluntary Principles to Counter CSEA online*.
- International Telecommunication Union, *Guidelines for Industry*

Capability 16. Increased Transparency

What is it?

- Regularly publish transparency reports on detection and prevention of CSEA online with meaningful metrics, and ensure data is supported by explainable methodology and reviewed regularly.
- Honest appraisal of responses and prevention techniques to inform future work and efforts.
- Transparency around the innovation of tools and techniques, research, allocation of resources, collaboration with other key stakeholders, staffing and training are also key.

Why is it important?

- Measurable indicators and transparency of progress, as well as challenges, can both prevent and respond to the elimination of online child sexual abuse and exploitation.
- Transparency can respond to online child sexual abuse and exploitation, and help the removal of CSAM, as it can motivate other actors to learn from success and initiate similar methodologies (where relevant) to reach the same end. It can also encourage collaboration between like-minded organisations to strengthen areas where there may be challenges or gaps.
- Transparency can prevent online child sexual abuse and exploitation, and help the reduction of CSAM, as it can highlight successes of collaboration and industry-wide, principled action and create doubt, increase risks or reduce potential action of offenders.

How can it be implemented?

- Organisations can share general successes and challenges in various formats and locations so as to reach all core audiences, including children and parents. Sharing channels can include their organisational websites, across various information-sharing fora with other actors working to eliminate online child sexual abuse and exploitation, in formats and spaces that are accessible to children and in formats and spaces that may be accessed by potential offenders.
- In some instances, the sharing of detailed methodologies to reduce CSAM may need to be kept private between collaborating organisations to prevent groups of offenders working together to identify techniques to overcome the successful methodologies.
- Protocols for sharing detailed methodologies across organisations and countries, with agreed data protection, security and confidentiality agreements, can be developed to ensure sharing of detailed methodologies. For example, this could be done between vetted organisations or between organisations who are members of WeProtect Global Alliance.

Further resources:

- Technology Coalition, *Project Protect*.

GSR Theme: Societal

Capability 17. Digital culture development

What is it?

- A demand for online child safety to be prioritised, whilst maintaining the right of children to privacy. Safety should be seen on a equal footing with privacy and security considerations. This should be built into technology and evolve with the online environment as they change. Increased public/citizen understanding of their rights and accountability of governments and companies of how they are upholding their responsibility and duty of care to children.

Why is it important?

- Digital culture outlines how humans interact online and how humans behave, think and communicate in an online society. Digital culture also reflects how humans understand and interact with persuasive technology (e.g. sharing, liking, profiling), misinformation and open online access and exploration (see capability 14).
- The rights and responsibilities of all actors and individuals must be respected online as they are offline; this is particularly important for children as childhood itself, and the various cognitive stages, has inherent vulnerabilities.
- It is also important for global citizens to understand the duty of care and associated responsibilities that technology businesses have towards them and to be able to hold technology to account when products or services are deemed harmful or unsafe for children.
- Due to the particular nature of the online environment it is possible for children (and adults) to remain anonymous or have fake profiles and that children may not always know who they are engaging with, even on a child-focused product or service. It is also possible for children, and adults, to keep their behaviour and communication and the services or products that they access and use private. When online children may have access to products and services with adult content, this is less common offline.
- All actors, organisations and individuals in society who engage with the online environment should understand children's online safety dynamics and need to be able to identify concerns, promote and support reasonable child safety features and act in a protective manner online where necessary.
- It is important therefore to develop and teach all individuals, and particularly children, their responsibilities and how to utilise digital environments in a responsible and safe manner.

How can it be implemented?

- Create a targeted, coordinated and widespread government campaign on what responsible digital engagement is (and is not), why responsible digital engagement is important, what individuals' responsibilities are in ensuring safe, pleasant and healthy digital engagement and how individuals can help to create a safe, pleasant and healthy digital engagement.
- The campaign should target different users, aiming to reach children of all ages, parents, adult digital users, technology industry and government representatives. Content, communication channels and key messages will need to be appropriate and relevant to specific audiences, representative user participation and intersectional analysis will be important to ensuring the campaign is relevant, inclusive and reaches diverse audiences.
- The campaign should aim to build moral responsibility, accountability and online social capital amongst all individuals and actors: how to be a good digital citizen. Information on the importance of reporting abuse or concerns of abuse should also be included in an aim to increase proactive reporting and responsible online communities.
- Include in the campaign a clear explanation that there are consequences based on online action and behaviour and, where possible or necessary, put in place disciplinary procedures (potentially offline) for bad behaviour.

Further resources:

- BBC, *Own It*.
- Childnet, *Parents and Carers Toolkit*.
- eSafety Commissioner (Australia), *eSafety Training*, *Parents and Carers*, *Start the Chat - Safer Internet Day*
- Global Digital Citizen Foundation, *Digital Citizenship School Programme*.
- Family Lives (UK), *Parent Channel TV*.
- Google, *Be Internet Awesome*.
- LEGO, *Small Builds for Big Conversations*.
- O2 and NSPCC, *Keeping kids safe online*.
- Report Harmful Content, *Helping Everyone Report Harmful Content Online*.
- SafeToNet Foundation, *Advice and Guidance*.
- Stop It Now! UK and Ireland, *Stop It Now: Helping Prevent Child Sexual Abuse*.
- ParentsProtect website (www.parentsprotect.co.uk)
- Telecommunication Development Sector (ITU-D) (2020), *Child Online Protection Guidance note*, Separate documents available in different languages for children; parents; industry; and policy makers.
- Young Minds, *Mental Health Support*.

Capability 18. Informed media reporting

What is it?

- Ethical, balanced and informed approach, a consistent use of terminology and a positive inclusion of victims / survivors, where appropriate.

Why is it important?

- Accountable, ethical and well-informed reporting of instances, trends or prevalence of abuse and exploitation, as well as its impact, is crucial to avoiding further harm or increasing risks for children.
- Unethical and inaccurate reporting could lead to re-traumatisation of the abuse for the victims or survivors and their families, or to the identification of the victims or survivors and their families and subsequent or further abuse, exploitation, stigma or discrimination.
- Unethical and inaccurate reporting could lead to the publication and further exploitation of risks, such as sharing online or in person access routes to children or potentially harmful gaps in products or services.
- Unethical and inaccurate reporting could lead to misrepresenting or generalising the issues, dynamics and trends behind online child sexual abuse and exploitation. Moreover, shame and victim-blaming (intentional or unintentional, through phrasing and content) can lead to a reduction in reporting.
- Inaccurate terminology could lead to the exclusion or double counting of particular risk groups or categories of children. It could also lead to misunderstandings or generalisations of the dynamics of abuse and risks for specific groups of children, e.g. children of a particular age, gender, race.
- Inaccurate terminology could also lead to misunderstandings on the potential level of harm of a risk or trend or misinterpretations of the abuse dynamics and therefore required prevention and response. (See capability 4).

How can it be implemented?

- Organisations and individuals working to eliminate online child sexual abuse and exploitation need to set the terminology and standards to guide the media and others in their reporting. This could be led by an international coordination body and agreed and implemented by a range of interested actors. (See capability 4).
- The media should be guided by a rights based approach and children's best interests as outlined in international commitments, including the UNCRC, Optional Protocol on the sale of children, child prostitution and child pornography, and the forthcoming UN General Comment on children's rights in relation to the digital environment. (See capability 3).
- Where technical disagreements remain or terminology compromises are challenging, clear standard explanations can be agreed. Where possible, decisions should be made on the general understanding that agreed international terminology is a central part of effective collaboration and coordinated and successful programmes.

- It is also important to avoid over reliance on figures and prevalence of types of abuse when we know that abuse is happening: one child victim of online sexual exploitation or abuse is enough to require action. Accurate numbers of the categories of children who are victims or survivors of online abuse or exploitation are, largely, unattainable. Due to a range of issues including stigma, fear of repercussions, lack of access or knowledge on reporting and lack of trust in the report procedure process and resulting action, it is likely that online abuse incidents are underreported and that real figures are likely to be higher than those reported and presented. The extent of reporting and underreporting is unknown. Simultaneous focus should be on the risks and potential harms that face children and in preventing and responding to those. (See capability 5).

Further resources:

- End Violence Against Children Partnership (2019), *Ending Violence Against Children: Key messages and statistics* (full version).
- Ethical Journalism Network, *Media and Trafficking in Human Beings Guidance note*.
- Interagency Working Group on the Sexual Exploitation of Children (2016), *Terminology Guidance note For the Protection of Children From Sexual Exploitation and Sexual Abuse*.

Capability 19. Restriction of children's exposure to illicit and harmful content online

What is it?

- Systemic restrictions and education to prevent child access to illicit content.

Why is it important?

- With open access to exploring the internet, and the vast amount of information it offers, children can be exposed to content that is sexually explicit, extremely violent or inappropriate for their age and cognitive and development stage. Other potentially damaging content can include sites which encourage or normalise harmful behaviour such as eating disorders, self-harm or terrorism, age inappropriate social networks, playing games and using apps that are not age-appropriate, joining unregulated chat rooms and watching livestreams which may show inappropriate content or may result in a child to taking part and being exploited without them knowing.
- Exposure to content that is inappropriate can be psychologically damaging. Moreover, such exposure can be frightening, confusing and difficult for a child to comprehend or balance. In some instances such exposure can also normalise harmful behaviour.
- Open access to the internet may expose children to potential contact with strangers, this can include adults and children using a false profile and/or adults and children who may have harmful intentions.

How can it be implemented?

- In analysing online restrictions, it is important to remember the benefits and opportunities of online access for children (see capabilities 2 and 3) and the importance of building an evidence base. The focus in implementing restrictions should be on enabling children to have healthy, safe and empowering access to quality digital products and services.
- Age-based restrictions, including age-verification, and control settings can be built into products and services, requiring parental or caregiver consent if necessary prior to registration and purchases. Methods to mitigate efforts to bypass control settings and to manage potential false profiles (e.g. a child or adult using a wrong date of birth or providing false details for consent) should be explored at the design stage (see capabilities 14 and 15).
- Specified parental controls and filters can be utilised to block access to particular products or services and manage the content that children search for online. Time limitation controls can also be added.

Further resources:

- Childnet International, *Parental Controls*.
- eSafety Commissioner (Australia), *Online Safety Basics*.
- eSafety Commissioner (Australia), global *Safety by Design* initiative.
- Internet Matters, *Parental Controls*.
- Information Commissioners Office (UK) (2020), *Age-appropriate design: a code of practice for online services*.
- Open Access Government, *How the government can protect minors online in a post-pandemic world*.
- UNICEF, *Investigating risks and opportunities for children in the digital world*

Capability 20. Education and outreach

What is it?

- Regular messaging through accessible channels that are appropriate to age, gender, race, disability, culture and nationality / language.

Why is it important?

- Methods to restrict content (see capability 19) will likely not 100% safeguard children from inappropriate content and exposure to potential contact with strangers. Children and other internet users need to be made aware of national laws, guidelines and the potential implications of sharing sexual content of themselves or others.
- Children, parents and caregivers, and the public in general need education on safe and responsible digital use so that they are aware of the risks, know what is expected of them and can respond appropriately to negative situations or harmful or inappropriate content (see capability 17).

- The skills and competencies that users need to be able to participate as responsible digital citizens are not acquired automatically and need to be learned and practised; education in this area is vital.[18]

How can it be implemented?

- Research on the risks and use of digital products and services, and how children uphold their rights and responsibilities online, can inform outreach and education services (see capability 23). Vulnerability assessments, with intersectional analysis, can also be carried out to understand the vulnerability of different groups of children to online sexual abuse and exploitation. With an understanding of the risks and vulnerabilities, educational content and information outreach can be developed in a way that is appropriate, understandable, relevant, participatory and inclusive for the population groups being targeted.
- Some core areas to cover in education content include: (i) competent and positive engagement with digital technologies, e.g. digital literacy (inclusion, access, creating, learning, working, communicating, playing), (ii) active and responsible participation in global online communities (rights, responsibilities, ethics, health, values, attitudes, intercultural engagement, community engagement, e-presence, ways of communicating) and (iii) balancing digital and offline worlds (safety and risks, wellbeing, privacy, informal vs formal settings, consumer awareness, evaluating content).[19]Social and emotional learning concepts should also be included in online safety education in order to support children in developing their social and emotional skills to engage in respectful online relationships and strengthen resilience.
- Core educational and outreach messages targeting different audiences should be aligned and based on evidence. A range of channels can be used to disseminate the education and outreach messages (online and offline formal / in a classroom, online and offline informal) material to target audiences. Children, parents and caregivers, teachers and the general public should be primary targets for the educational content.

Further resources:

- BBC, *Own It*.
- SafeToNet, SafeToNet
- Childnet, *Parents and Carers Toolkit*.
- Council of Europe, *Digital Citizenship and Digital Citizenship Education*.
- Council of Europe, *Digital Citizenship Education Handbook*.
- eSafety Commissioner (Australia), *eSafety Training*, *Best Practice Framework*, *Toolkit for Schools*
- eSafety Commissioner (Australia), *Protecting voices at-risk online*.
- Everfi, *Ignition: Digital Literacy Curriculum for Wellness and Safety*.
- Family Lives, *Parent Channel TV*.

18 – Informed by: Council of Europe, *Digital Citizenship and Digital Citizenship Education*.

19 – Informed by: Council of Europe, *Digital Citizenship and Digital Citizenship Education*.

- FBI (US), *Safe Online Surfing*.
- Google, *Be Internet Awesome*.
- LEGO, *Small Builds for Big Conversations*.
- Microsoft, *Digital Literacy Course*.
- O2 and NSPCC, *Keeping kids safe online*.
- Report Harmful Content, *Helping Everyone Report Harmful Content Online*.
- Stop It Now, *Stop It Now: Helping Prevent Child Sexual Abuse*.
- Young Minds, *Mental Health Support*.

Capability 21. Offender outreach

What is it?

- Develop targeted early intervention strategies to reach those at risk of offending and develop targeted strategies to reach existing offenders and signpost to sources of help to change behaviour.

Why is it important?

- Understanding the characteristics, dynamics and motivations for abuse in general, including CSEA online, is crucial to developing effective strategies aimed at its elimination. This includes understanding risk profiles and behaviours. For some come children and young people, engaging in harmful sexual behaviours may be associated with experiences of trauma, sexual or physical abuse, discrimination, disadvantage or exposure to violence.
- Strategies targeting (i) individuals at risk of offending and (ii) existing offenders can obstruct irrational decision-making processes and provide advice and information, including on legislation and criminal justice implications. Strategies should aim to prevent an individual from deciding to offend or re-offend.
- Increases in demand for CSAM, and online child sexual abuse and exploitation more generally, require increases in supply. Reducing, or eliminating, the demand is one logical and important component of a global strategy.

How can it be implemented?

- Detailed research and analysis can be carried out to understand who is at risk of offending and who is actually offending, why, how (through what digital channels and offline methods) and where they are physically located. It is also useful to understand how offenders and potential offenders engage with each other and share techniques and methods. With a detailed understanding of the offending risks, dynamics and approaches, information and outreach strategies can target different groups of potential and existing offenders. (See capability 24).

- Specific capacity building, including training and mentoring, for service providers, parents, teachers and others where necessary on understanding sexual offenders can be provided.
- Information can be disseminated to child protection actors on legislation and criminal justice implications relating to child sexual abuse and exploitation.
- Anonymous helplines can be set up, or a service extended to existing helplines, to reach anyone "concerned about their own thoughts or behaviour towards children; those worried about the sexual behaviour of another adult, or a child or young person; or any other adult with a concern about child sexual abuse including survivors and professionals".
- Comprehensive monitoring and evaluation, and academic research where possible, should be built into approaches and strategies to ensure that lessons are learned on successes and challenges, which can be shared and, where successful, replicated

Further resources:

- The Lucy Faithfull Foundation, *Services*.
- Stop It Now! UK and Ireland, *Stop It Now: Helping Prevent Child Sexual Abuse*.
- The Lucy Faithfull Foundation/Stop It Now! UK and Ireland, *online deterrence*
- Australian eSafety Commissioner, *Harmful sexual behaviours*

GSR Theme: Research and insight

Capability 22. Threat analysis and monitoring

What is it?

- Detailed and up-to-date assessments of defined threats, risks and trends.

Why is it important?

- Children face a range of individual and combined threats and risks[20], including those relating to sexual exploitation and abuse, when interacting online. The threats and risks can manifest online and offline and come from a range of actors and settings. Systematic and coordinated identification, monitoring, management and mitigation of all threats and risks is crucial to strengthening the safeguarding of children online and offline and to reducing the possibility of unintended (or intended) harms coming to life.
- Threat analysis and management and risk management are standard good practice in (offline) project management and operations. Therefore, all actors planning, delivering, supporting, strengthening and advocating to change a specific online or digital project should also uphold their responsibility to identify and manage the associated threats and risks.

How can it be implemented?

- Targeted research projects (long-term / 5+ years or longitudinal where possible) with a baseline and pre-set, relevant and appropriate indicators, and both qualitative and quantitative research tools, should be established to monitor and analyse threats, risks as well as the opportunities for different groups of children.
- Where possible, and not in contravention of confidentiality or privacy legislation, intersectional analysis should be integrated into the research. This is key to being able to design effective programmes that actually prevent and respond to the identified threats and risks.
- Input from different groups of children and stakeholders with varied expertise (e.g. technology engineers, criminal justice staff, and child protection professionals) across organisations, sectors and countries will strengthen the research quality.

Further resources:

- CO:RE, *Children Online : Research and Evidence*.
- Independent Inquiry: Child Sexual Abuse (Wales), *Rapid Evidence Assessment: Quantifying the Extent of Online Facilitated Child Sexual Abuse*.
- LSE, *Global Kids Online*.
- LSE, *EU Kids Online*.
- UNICEF Innocenti, *Global Kids Online*.

20 – Risk is defined here as a chance or possibility that an individual will be harmed.

Capability 23. Research to understand children's online vulnerabilities and effective safety education systems

What is it?

- Online safety and preventative approaches.

Why is it important?

- Understanding children's online vulnerabilities to sexual exploitation and abuse is key to designing relevant, appropriate and targeted safety education material and systems.
- Understanding vulnerabilities can also help inform more effective prevention and response programmes and initiatives.

How can it be implemented?

- Research and analysis needs to consider who, how, where and why children are more or less vulnerable to sexual abuse and exploitation online, and if, when, where and how that changes over time. (See capability 22).Effective safety education systems need to be evidence-based and appropriate to the target audience. (See capability 20). Online safety education should be based on recognising, acknowledging, and understanding rights and responsibilities in the digital age. This should:
  - Focus on students in the context of their relationships with, and responsibilities to, others.
  - Uphold children's rights to provision, participation and protection in digital environments.
  - Acknowledge the significant opportunities and safety challenges that students face in online environments.
  - Empower all students to participate meaningfully in the design, development, and implementation of their online safety education, where appropriate

Further resources:

- CO:RE, *Children Online : Research and Evidence*.
- Independent Inquiry: Child Sexual Abuse (Wales), *Rapid Evidence Assessment: Characteristics and Vulnerabilities of Online Facilitated Child Sexual Abuse and Exploitation*.
- LSE, *Global Kids Online*.
- LSE, *EU Kids Online*.
- UNICEF Innocenti, *Global Kids Online*, *Disrupting Harm*
- UNICEF, *2021 Rapid Evidence Review*
- Australian eSafety Commissioner, *Best practice framework for online safety education*
- Disrupting Harm,

Capability 24. Offender Research

What is it?

- Offender behaviour, drivers, pathways and effective interdiction.

Why is it important?

- Understanding the characteristics, dynamics and motivations for abuse in general, including CSEA online and other online harms, is crucial to developing effective strategies aimed at elimination. This includes understanding who the offenders and potential offenders are (male, female, adult, child) and where they are based.
- Strategies targeting (i) individuals at risk of offending and (ii) existing offenders can be based on research / understanding of thought processes and strategies behind online sexual exploitation and abuse. Based on relevant evidence, strategies can aim to prevent an individual from deciding to offend or re-offend. (See capability 21) and setting societal standards for online behaviour will help some people to not offend in the first place.

How can it be implemented?

- Detailed research can identify and analyse who is at risk of offending and who is actually offending, why, how (through what digital channels and offline methods) and where they are physically located (as many cases are cross-border).
- It is also useful to understand if, where, why, and how current, potential and previous offenders engage with each other and share techniques and methods.
- It is important to include current, potential and previous offenders in any research design to understand the dynamics and decision-making rationale. This should include research and analysis of "demand and supply" routes and the role of intermediaries or organisers (who can often be family members of the victim or survivor).

Further resources:

- Centre of Expertise on child sexual abuse, *Key messages from research on child sexual abuse*.
- Independent Inquiry: Child Sexual Abuse (Wales), *Rapid Evidence Assessment: Behaviour and Characteristics of Online Facilitated Child Sexual Abuse and Exploitation*.
- *LFF/Stop It Now! IIOC Deterrence campaign and resources.*
- Stop It Now! US, NL, Flanders and UK& Ireland reports; plus Dunkelfeld.
- NCA "Pathways" research.

Capability 25. Long-term victim trauma analysis

What is it?

- Mental health, societal and economic.

Why is it important?

- Long-term analysis of the personal implications (e.g. health, economic, social, education) of being a child victim or survivor of online sexual abuse and exploitation is crucial for two core reasons: (i) it can inform targeted immediate and long-term support services, and (ii) it can be used as evidence for campaigning, advocacy and policy and systems change, particularly targeting the government and technology industry actors. (See capabilities 9, 10, 11, 12).
- Similarly, long-term analysis of the societal implications (e.g. education attainment, economic development, social interactions, community dynamics) of having a range of child victims or survivors of online sexual abuse and exploitation across the globe can inform: (i) immediate and long-term social support and online safety education programmes and services, and (ii) campaigns, advocacy and policy and systems change, particularly targeting the government and technology industry actors. It can also help target future resources towards those worst affected and equip parents/caregivers to play their best role in aiding recovery.

How can it be implemented?

- Targeted research projects (long-term / 5+ years or longitudinal where possible) with a baseline and pre-set, relevant and appropriate indicators, and both qualitative and quantitative research tools, should be established to monitor and analyse implications over the long-term or reflect back on changes over time.
- Where possible, and not in contravention of confidentiality or privacy legislation, intersectional analysis should be integrated into the research. This is key to being able to design effective programmes that actually prevent and respond to the identified threats and risks.
- Input from different groups of children and stakeholders with varied expertise (e.g. economic, social welfare, and education professionals) across organisations, sectors and countries will strengthen the research quality.

Further resources:

- Centre of Expertise on child sexual abuse, *Key messages from research on child sexual abuse*.
- Child Welfare Information Gateway (US Government), *Social and Economic Consequences of Child Abuse and Neglect.*
- ODI (2014), *The costs and economic impact of violence against children*.

Capability 26. Ethical AI and Innovation

What is it?

- Increased and sustained investments in ethical AI and safety-enhancing solutions.

Why is it important?

- Due to the prevalence of existing CSAM online, and the likely extent of undetected CSAM on the dark web, technology needs to make rapid and extensive progress to identify and remove the existing levels of CSAM online as well as to prevent new cases and respond to active cases.[21](See capabilities 13, 14, 15, and 16).
- Also, methods to access different children and to commit CSEA online are ever changing and evolving. Offenders are likely to collaborate and share methodologies and tactics to bypass safety mechanisms and to share vulnerable profiles or existing abusive content.
- Similarly, on some sites, profile types can be recommended to those who have shown a prior interest in children – in some cases this will be recommending children to adults.[22]

How can it be implemented?

- Carry out research and identify innovative practice to "*build crucial technological tools needed to more effectively prevent and work to eradicate child online sexual exploitation and abuse*"[23] including deterrence for offenders.

Further resources:

- eSafety Commissioner (Australia), global *Safety by Design* initiative.
- Lucy Faithfull Foundation, *Services*.
- 5Rights Foundation, *Risk-by-Design microsite*.
- Technology Coalition, *Project Protect*.
- Thorn, *Safer*.
- SafeToNet, SafeToWatch

21 – End Violence Against Children, *Safe Online*.

22 – 5Rights Foundation, *Risk-by-Design microsite*.

23 – Technology Coalition, *Project Protect*.