वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE

G20 TOOLKIT

on Cyber Education and Cyber Awareness for Children and Youth

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This toolkit was initiated and published by the Indian G20 Presidency and Ikigai Law with support from the International Telecommunication Union (ITU) under the priority area, Security in the Digital Economy. With the aim to improve the security landscape in the digital economy through information sharing, the toolkit shares best practices developed by various G20 members and guest countries to promote cyber education and cyber awareness among children and youth.

This toolkit has been enriched by the active contributions of G20 members and guest countries with valuable information as part of the questionnaire used for preparing the following toolkit as well as inputs shared during the working group meetings and in writing. We sincerely hope that this toolkit will become a cornerstone of the G20's journey towards a safer digital future and pave the way for a sustainable, inclusive, and resilient digital economy.

EXECUTIVE SUMMARY

The close integration of digital technologies in the lives of children and youth has translated into various benefits in the way of access to information, increased connectivity to online spaces, and the opportunity to learn a wide array of skill sets. However, the surge in online activity has also led to a proliferation of cyber risks specifically targeting children and youth. This trend was also backed by our empirical findings based on the responses of the G20 members and guest countries to the questionnaire on security practices.

To mitigate these risks, G20 members and guest countries have adopted and implemented a broad range of measures. These include comprehensive regulations and capacity-building measures, such as the creation of dedicated websites and applications. This toolkit shares some such measures. We found that measures to further child online safety are based on a combined assessment of the following factors:

1. The type of risk
2. Targeted entity
3. Implementing stakeholder
4. Desired outcome

This toolkit depicts this approach in the pyramidal model but acknowledges that the adopted measures may vary from this approach as per the social, economic, political, and cultural contexts of a member. As a caveat, this structure is meant to be a broad overview of the information compiled and may not reflect all present approaches to online child safety.

Drawing from desk research and responses to a survey circulated by the Indian Presidency among all G20 members and guest countries, the toolkit shares five takeaways for policymakers to consider improving child online safety. These include:

1. Classifying risks and responses based on sub age groups: Given the diverse use-cases of the internet, children from different age and gender groups can be vulnerable to some online risks more than others. Therefore, more targeted cyber awareness and cyber education measures may improve their safety online.
2. Investing in response, referrals, and support systems: In addition to capacity-building measures, awareness, and legislative interventions, accessible response, referral, and support systems can be helpful if a child is experiencing online harms. Therefore, governments can consider investing in such support mechanisms and ensuring that they are easily accessible to children.
3. Adopting and investing in a multistakeholder approach throughout the decision-making process: To ensure that cyber awareness and cyber education programs are effective, it can be helpful for governments to adopt a multistakeholder approach and consult children while designing and implementing such programs.
4. Promoting global cooperation to further child online safety: Given the commonalities in the risks, actors and responses, countries may benefit from regular information exchanges and collaboration.
5. Critical role of businesses and online platforms: It is also important to note the role of businesses and online platforms where children and youth encounter the various online risks. Therefore, businesses and platforms have a responsibility to take proactive measures to improve security and protect young users.

PART ONE:
G20 Toolkit on Cyber Education on Cyber Awareness for Children And Youth

INTRODUCTION

Today, the digital environment is an integral part of the lives of children and youth and offers tremendous benefits by way of connectivity, information sharing, and increased access to and use of online spaces. United Nations' International Children's Emergency Fund (UNICEF) research suggests that one in three internet users is under the age of 18. However, UNICEF itself, along with a sizable body of literature surveyed in the *Mapping of Cyber Awareness and Cyber Education* section accompanying this toolkit, recognizes that this burst of online activity has led to the proliferation of online risks directed at children and youth which can have devastating consequences. Consequently, cyber education and cyber awareness for this demographic and the addressing of systemic and structural challenges to online safety has become a national policy priority for governments around the world.

International organizations such as the ITU have recognized the significance of this challenge and framed guidelines such as the ITU's Guidelines for policymakers on Child Online Protection, Guidelines for policymakers[1], and a related Policy Brief[2] as well as the Organisation for Economic Cooperation and Development's Recommendations on Children in the Digital Environment.[3] G20 members have explicitly acknowledged this challenge and opportunity. In 2021, the G20 Digital Economy Ministers declared their commitment by adopting the *G20 High Level Principles for Children Protection and Empowerment in the Digital Environment*[4]. To further this principled commitment, several G20 members formulated strategies, shaped regulations, and undertook cyber education and cyber awareness initiatives.

The overall aim of decision-makers should be to promote a safer online environment for children and young people. Linked to this, responses should be preventative and proactive - focusing on the overall digital ecosystem to promote greater education and resilience amongst children and young people in response to online harms. These measures should be deployed in addition to responses targeted at perpetrators of criminal activity. Responses should reflect the role of different stakeholder groups in promoting greater transparency, accountability and digital education and awareness.

Existing research, as surveyed in Part 2, suggests that children and youth are exposed to a range of risks of harm including exposure to and accessing inappropriate or harmful content, online fraud, sextortion, luring and grooming, identity theft, misinformation, and financial crimes. To address these risks, there are a range of policy interventions used by governments and other stakeholders, including legislative, policy, educational and awareness building measures. This toolkit endeavours to map and provide a broad overview of the online risks as well as interventions by governments and other stakeholders on cyber education and cyber awareness. Additionally, it provides key takeaways based on G20 members' initiatives addressing online risks to children and youth.

---

[1] ITU, "Guidelines for policymakers on Child Online Protection", 2020, https://www.itu-cop-guidelines.com/_files/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[2] ITU, "Keeping Children safe in the digital environment: The importance of protection and empowerment", 2021.

[3] https://www.oecd.org/digital/children-digital-environment/#:~:text .

[4] G20 Digital Economy Ministerial Declaration 2021. https://www.mimit.gov.it/en/g20-en

This document is divided into two sections. The first section provides an analytical structure illustrated through a response pyramid to explain and evaluate the data surveyed. It also outlines key takeaways based on G20 members' approaches and experiences. The mapping section surveys relevant academic and policy literature on the risks faced by the target demographic of children and youth. Following that, the toolkit surveys policy, and regulatory solutions as well as cyber awareness and cyber education measures undertaken by G20 members.

METHODOLOGY

The toolkit relied on three phases of research:

- Phase 1: Empirical desk-based research that reviewed a range of publicly available sources on G20 countries to map information relating to the core research questions.
- Phase 2: Consultation with G20 members and obtaining direct insights through a questionnaire circulated in February 2023. Nineteen G20 members and nine guest countries responded to the survey.
- Phase 3: Consolidation of data from mapping and consultation.

UNIQUE CONTRIBUTION

This toolkit makes two unique contributions to existing policy and literature:

1. Mapping of risks to children and youth identified by G20 countries: By evaluating data obtained through publicly available documents and insights from the questionnaire, the toolkit serves as a useful survey and mapping of information on the nature of risks to children and youth faced by advanced and developing digital economies.

2. A structure delineating state responses to risks: States have adopted a variety of interventions including top-down regulation as well as bottom-up or horizontal approaches including cyber awareness and cyber education initiatives. This toolkit is a first of its kind attempt at capturing the diverse approaches deployed by G20 countries in addressing online risks facing children and youth.

   The response structure shared in this toolkit can be used as a general starting point for governments, private sector entities, civil society organizations, and other stakeholders to consider some of these risks and examples of mitigation measures in relation to their needs and local contexts. The compilation of examples both in the toolkit and mapping sections are for information sharing only and not an endorsement of any particular approach.

LIMITATIONS

This toolkit is based on desk research including literature surveys and a review of publicly available documentation as well as questionnaires and interviews with policymakers. It did not rely on anthropological research methods such as interviews with children and youth or teachers to critique or test existing regulations or the various cyber awareness and cyber education interventions. In short, the purpose of the toolkit is not to evaluate existing policy measures or suggest new interventions, rather to understand the breadth of policy

responses and the role of different stakeholder groups in their design, development and delivery. The compilation of examples both in Part One and Part Two are for information sharing only and should not be treated as an endorsement of any particular approach.

The toolkit does not seek to prescribe a model for understanding as complex and multifaceted an issue as the online safety of children and youth. All policy interventions should take into account up-to-date evidence and research in a national and international context, and reflect the social, economic, political, and cultural contexts of G20 members - while ensuring the rights of children are promoted and protected in line with the United Nations Convention on the Rights of the Child, as appropriate. Consequently, the models highlighted in the toolkit provide, at best, a theoretical overview and are not intended to necessarily prescribe, define, or fully account for local circumstances.

DEFINITIONS

The definitions elucidated in this section are to be understood only with reference to the use of the terms in this toolkit. The objective of this section is not to provide authoritative and interoperable definitions of the terms. To clarify, the definitions in this section are intended without prejudice to definitions adopted by G20 members and observers.

- "Cyber education": Specific formal courses taught in educational institutions such as schools and colleges, targeted at children and youth.
- "Cyber awareness": General capacity-building programs targeted at students, parents, teachers, and law enforcement authorities conducted by governments, nongovernmental organizations (NGO), international organizations through both institutionalized and less formal mechanisms.
- "Children": Describes all persons under the age of 18 years.
- "Youth" (or young people): The United Nations, for statistical purposes, describes persons aged between 15 and 24 years of age. However, for the purposes of this paper, we refer to youth as persons aged 18-24, in order to ensure that this group is distinguished from the 'children' group. This is without prejudice to law and policy across jurisdictions that may categorize based on prevailing understandings and socio-economic implications.
- "Online Risks": Uncertainty about and severity of the consequences (or outcomes) of online activity by children.[5]

[5]Sonia Livingstone and Maria Stoilova, the 4Cs: Classifying Online Risk to Children. (Hamburg: Leibniz-Institut Medienforschuns Hans-Bredow-Institut (HBI); 2021) https://doi.org/10.21241/ssoar.71817

ANALYSIS:
A STRUCTURE TO ADDRESS RISKS

SUMMARY OF ONLINE RISKS

Drawing from the surveyed literature, the accompanying mapping section identifies risks to child online safety. Sources and citations are available in that section and a summary is provided below in Box 1:

1. Content

Content risks refer to situations "where a child or young adult is exposed to unwelcome and inappropriate content." Inappropriate content may be targeted towards the consumer or be mass produced.

- *Misinformation and disinformation*
  Misinformation often refers to false or misleading information that is unwittingly shared whereas disinformation is deliberately created with an intent to deceive or harm.
- *Hateful Content*
  Hateful content often refers to online hate speech that is expressed digitally through devices like computers and mobile phones. Hate speech attempts to spread and justify intolerance and discrimination based on ethnicity, religion, sexuality, disability and other factors.
- *Other harmful content*
  Exposure to harmful or age-inappropriate content online, including relating to pornography, may increase risks for poor mental health, sexism, and objectification.

2. Consumer

Consumer risks are risks faced by children and youth owing to their participation as consumers in the digital environments.

- *Fraud*
  Online financial scams and frauds may target individuals of any age, but youth are particularly susceptible.
- *Profiling*
  Commercial profiling, where data is used to create marketable digital profiles for advertising or other commercial purposes poses risk for all users that may be exacerbated in the absence of informed consent and may in some cases violate applicable consumer and/or data protection laws.
- *Risks to Data Privacy and Security*
  Lack of data privacy and security are specific risks for children and youth as there may be lower level of understanding of these risks compared to other age groups.

3. Conduct

The child witnesses, participates in, or is a victim of potentially harmful conduct by themselves or other children online.

- *Extensive unbalanced screentime*
  All over the world, children are spending increasing amounts of time on the internet, causing parents and caregivers to fear that they are missing out on real world experiences. There are other risks, too,

including physical health risks, mental well-being, and insomnia.

- *Cyberbullying*
  Cyberbullying is bullying through the use of digital technologies such as social media platforms, messaging or chat platforms and gaming sites.
- *Intimate image abuse*
  Intimate image-based abuse takes place when an individual leaks or threatens to leak an intimate image of a child or youth without their consent.

4. Contact
   Contact risks are defined as risks that the "child experiences or is targeted by contact in a potentially harmful adult-initiated interaction, and the adult may be known to the child or not."[6]

- *Grooming and luring*
  Process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person. Use of applications and platforms to connect with children and youth for the purpose of sexually exploiting them.
- *Online child sexual abuse and exploitation*
  Child sexual abuse or exploitation that is partly or entirely facilitated by technology, including the creation and sharing of child sexual abuse material (CSAM).
- *Online sexual encounters*
  Children could face a range of other online sexual encounters that are not initiated for the purpose of creating CSAM.
- *Sextortion*
  Sextortion is a form of blackmail in which the perpetrator threatens to reveal sexual materials about the victim in exchange for money or further sexual materials. [7]

All G20 members surveyed recognize the significance of cyber risks to children and youth. The 4Cs classification used in the surveyed literature is a useful typology to evaluate each risk and provide solutions. However, it should be noted that the same sequence of events can manifest itself as multiple types of risks. For example, cyberbullying is a contact risk if perpetrated by an adult; a conduct risk if perpetrated by a child; and a content risk if the content responsible for bullying remains openly available on social media.

G20 members have adopted a range of measures to promote child online safety. The details of this are provided in the accompanying mapping section. The following section suggests a structure for conceptualising the solutions and responses surveyed.

[6] https://www.netsweeper.com/filter/education-web-filtering/the-4cs-of-online-safety-part-2-what-is-online-contact-risk/35967
[7] https://www.cybertip.ca/en/online-harms/sextortion/

STRUCTURE AND RESPONSE PYRAMID

The objective of measures taken by the government or by other stakeholders is to create a safer online experience for children and young people. Given that risks vary in relation to online platforms and the actors involved, a one-size-fits-all model will not work - responses should focus on ensuring children and young people are empowered to safely navigate the digital environment, and online platforms have adequate systems and processes in place to address key risks to children and young people online. All stakeholders should be encouraged to promote greater transparency and accountability in the design, development and delivery of online safety responses and platforms' systems and processes.

After collecting and processing publicly available data gathered through desk research along with data provided in the questionnaires, the inverted pyramid[8] and corresponding table (Table 1) can serve to illustrate measures undertaken by G20 members and observers on this issue. This response pyramid provides a simplified overview[9] of the measures undertaken by G20 members as outlined in Part Two of the document; it is not an endorsement of specific measures or approaches taken in different jurisdictions nor as an overall approach for structuring policy responses. The G20 members recognise the importance of multifaceted, multi stakeholder approaches, including ensuring platform responsibility and accountability, which will vary according to the local circumstances, with the overall aim of ensuring a safer online experience for children and young people.

As shown in Table 1, the decision on an action/measure (Column E) to address risks is taken by decision-makers after a combined assessment of the following factors:

1. The type of risk (as depicted in Column A)
2. Targeted entity or group (as depicted in Column B)
3. Implementing stakeholder (as depicted in Column C)
4. Desired outcome (as depicted in Column D)

The structure of the pyramid recognizes that furthering online safety and resilience is a holistic endeavour that should always be a multistakeholder and multidisciplinary effort. These efforts often include education, awareness, and capacity-building and may be accompanied by regulatory measures focused on ensuring greater transparency and accountability from online platforms and sanctions for perpetrators of harmful criminal activity (e.g. CSAM).

- At the first level, there are two measures that reflect the need for a holistic approach to online safety that includes a range of stakeholders . These measures include:
    - Systemic capacity-building and awareness, in which the targeted stakeholders are parents, guardians, teachers, and law enforcement authorities and other actors who interact on behalf of and

[8] Adopted from Ayers and Braithwaite, Responsive Regulation: Transcending the deregulation debate: http://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf

[9] Desk research shows that all G20 members have either implemented or are developing measures at all three levels of the pyramid. Specific responses to questionnaires suggested that a significant number of G20 members (11 out of 19 responses) are conceptualizing measures at all three levels. The relational pyramid is an attempt by the Presidency to theoretically capture these approaches at a very high-level. The structure does not necessarily reflect the declared approach of any G20 member or capture the range of approaches that G20 members and observers may adopt and implement. It is also not an endorsement of one particular approach nor a prescriptive model for G20 members or other jurisdictions.

in the best interest of the child and the implementing stakeholders are governments, civil society organisations, non-governmental organisations (NGOs), and international organisations (IOs). The desired outcome is to promote greater education and awareness amongst stakeholders that work around children and impart best cyber awareness and cyber education practices so as to enable them to proactively detect and mitigate risks faced by children and youth.

  - Cyber education and awareness specifically targeted at children wherein the implementing stakeholders are governments, regulators, NGOs, educational institutions, online platforms, and the objective is to nurture healthy online behaviour among children.

- At the second level, there are platform duties and responsibilities including the identification of risks to children and setting up transparent, accountable, and proportionate measures to deal with these risks. Platforms and businesses are crucial stakeholders for furthering online child safety.[10]

- At the third level, there are potential regulatory requirements and corresponding enforcement measures for non-compliance. These measures should predominantly be deterrents aimed at promoting greater accountability and compliance from online platforms. Such measures can include fines, blocking measures, or senior management liability in case of failure to provide required information to regulatory bodies or to take the necessary steps to address the most egregious forms of harmful online activity on their platforms (e.g. CSAM). Criminal enforcement measures could also target deterring malicious behaviour. Such measures can be implemented by governments for the purpose of deterring future malicious activity.

We recognize that this pyramid is a simplified structure and will not account for all decision-making challenges or policy decisions. It instead serves as a potential guide for decision-makers to adopt based on local context.

[10] Suggested by the United Kingdom.

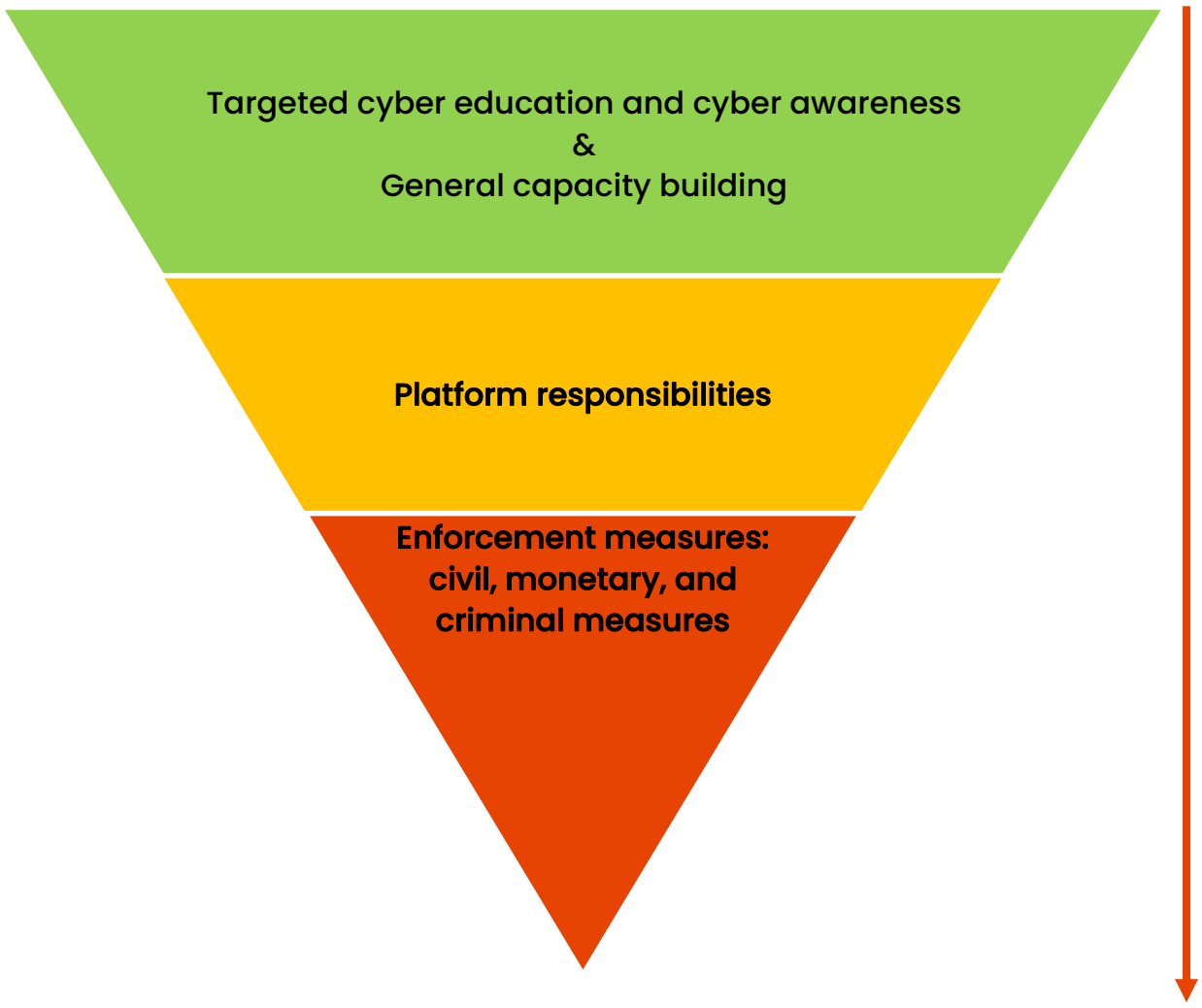

Figure 1: Response pyramid to address online risks to children and youth.

Risks covered (Column A)	Targeted entity or group (Column B)	Implementing stakeholder (Column C)[11]	Desired outcome (Column D)	Type of action/measure (Column E)
Preventive measures for all risks	Children and youth	• Governments, • International Organizations • Online platforms • Law enforcement agencies, • Parents • Educational institutions	Preventative measures to nurture healthy online behaviour	Cyber education
Preventive measures for all risks	• Educational institutions, • Teachers, parents and guardians • Law enforcement agencies, • Online platforms	• Governments • Regulators, • International Organizations • Non-Governmental organizations • Platforms	Preventative measures to create a nurturing ecosystem for children and youth	Cyber awareness and capacity building
Risks determined by platforms and other implementing stakeholders	Online platforms	• Governments, • Online platforms and independent regulators with inputs from and auditing by stakeholders such as civil society organizations	Proportionate, transparent, and accountable systems and processes to address risks to children online; ensuring greater accountability and transparency in the design, development and operation of online platforms.	Platform responsibilities[12]
Harmful activities such as child sexual abuse and exploitation material	Malicious actors	Governments, including law enforcement	Deterrence and accountability	Enforcement measures, including civil and criminal legislation

Table 1: Structure for measures to address online risks to children and youth.

[11] Note that even as implementing stakeholders changes at each level, G20 members usually have stakeholders such as academia involved in the consultation process and devising of specific actions/measures

[12] This could take the form of self-regulation or voluntary codes of conduct.

KEY TAKEAWAYS

In addition to the overarching decision-making structure identified in the previous section, the following section lists key takeaways from G20 members' experiences when conceptualizing and implementing cyber awareness and education programs for children and youth.

CLASSIFY RISKS AND RESPONSES BASED ON SUB-AGE GROUPS

The Indian G20 Presidency's desk research and questionnaires revealed that very few countries maintain data on the nature of risks faced by age groups within the broader category of 'minors.' There is no distinction made between children aged 5-12 years (broadly elementary school), 13-18 years (broadly middle and high school) and youth aged 18-21 years (college students). In fact, apart from India, very few countries have mandatory cyber education courses for college students (youth) regardless of their field of study. Most university curricula on cyber awareness and cyber education are geared towards producing cyber security professionals.

However, in response to the circulated questionnaire, nine G20 members and seven guest countries provided initial evidence and thinking on how risks can be separated by age group. Policymakers should also consider developing policy measures that specifically protect girls online as they may be subject to more severe or differing forms of abuse.[13] Collecting data and using gender-disaggregated data may help to counteract inequalities and intersectional discrimination.

The nature of risks faced by and consequently the intervention needed to mitigate those risks do not apply across the board to all sub-age groups equally. While there is little publicly available empirical evidence to back this, some responses to the Indian G20 Presidency's questionnaire shared some initial reasoned thinking on how risks may materialize differently to the specified sub-groups. The table below aggregates some of this information but does not reflect a complete account or endorsement of the same:

GROUP	RELEVANT RISKS
Primary school students aged 5-12 years	Potential exposure to unsuitable content such as streaming, audiovisual media, and games are risks for this group. Contact risks such as cyberbullying and other forms of manipulation and child sexual exploitation are possible but less likely if online access is more closely monitored by parents and caregivers. However, this situation may be changing. For example, research during COVID demonstrated that children aged 5-12 years became even more active online, with minimal or no supervision. Further, consumer risks, such as susceptibility to profiling and privacy violations, are also possible for this group. .[14]
Middle and high school students aged	As online use increases, interactive risks such as contact, conduct

[13] Suggested by the Republic of Oman and Germany
[14] Input received from Canada

12-18 years	and consumer risks become more prevalent. Given less parental control, children are also prone to more manipulation, sexual exploitation, and bullying. Content risks also can be a risk for this group.
Young people (18-24 years)[15]	Youth have more financial independence than school going minors and are consequently more prone to consumer risks. Young people also may be vulnerable to content risks However greater maturity means that they are less likely to be exploited or manipulated through contact or conduct risks.

1. INVEST IN RESPONSE, REFERRALS, AND SUPPORT SYSTEMS

In addition to capacity-building measures, awareness, and legislative measures, proactive investment is important in accessible response, referral, and support systems that children experiencing any harm can access. Law enforcement officials and child support agencies can be empowered and trained to act as first-responders and provide the necessary grievance redressal and other forms of mental support in response to an incident. It is important that support mechanisms are easily accessible to all children. Therefore, approaches need to be designed with a gender sensitive and inclusive approach.

Existing practices on how to harness technology may be considered to facilitate said support mechanisms often involve multi-stakeholder collaboration with support from government. Some instances of such technology facilitated support mechanisms are listed below:

- Türkiye also has a hotline that individuals can report any harmful content they come across through a website. The website allows reporting under eleven categories including sexual exploitation of children and is a member of the International Association of Internet Hotlines.[16]
- Canada, under the National Strategy for the Protection of Children from Sexual Exploitation on the Internet The Canadian Centre for Child Protection (C3P) is an organization dedicated to reducing child victimization by providing national programs and services to the public. They are responsible for the operation of Cybertip.ca, where Canadians can report suspected cases of online sexual exploitation of children. With support from Public Safety Canada, C3P also manages Project Arachnid, an automated web crawler that detects and processes tens of thousands of images per second and sends take down notices to online service providers to remove child sexual abuse material globally. The accompanying mapping section surveys other such approaches adopted by G20 members.

2. ADOPT AND INVEST IN A MULTISTAKEHOLDER APPROACH THROUGHOUT THE DECISION-MAKING PROCESS

The diverse array of risks and range of mitigation options means that a multistakeholder approach is key. In a

[15] Not with prejudice to countries that consider anyone aged 18+ an adult and consequently outside the remit of this toolkit or this framework
[16] https://www.ihbarweb.org.tr/eng/index.html

whole of society approach to child online safety, many stakeholder groups are involved in the design, delivery and deployment of policy measures and leverage their diverse experience, expertise, and resources to develop comprehensive policy solutions. G20 members have recognised the relevance of other stakeholders in designing and implementing regulations, cyber awareness and cyber education measures.[17] Meaningful multi-stakeholder inputs are important at every stage through extensive consultation. Children's rights in the digital environment, as set out in the Office of the High Commissioner for Human Rights (OHCHR) General Comment No. 25, must be protected through the range of online safety measures developed and designed by different stakeholder groups.

It is also important for children to be actively involved in the co-development and design of online safety initiatives - for example, through peer-to-peer education programmes. Technology driven solutions for grievance redressal and information sharing should be considered.

Further, a robust multi-stakeholder ecosystem can benefit from coordination within government ministries and departments such as child welfare, health, and law enforcement at all levels of the state. It is suggested that members invest earmarked funds to grow a multi-stakeholder ecosystem.

Several stakeholders have a role to play in furthering child online safety, as shown in the table below:

Stakeholder	Role
Law enforcement	Enforcement of criminal legislation as well as monitoring and detection of CSAM (in accordance with respective legal frameworks), and capacity building.
Regulatory bodies	Enforcement of regulatory requirements; promoting compliance with regulatory duties; coordination amongst public bodies with an interest in child online safety, for example, ICT, child development, welfare, and law enforcement.
Educational institutions (schools, colleges)	Develop and deliver comprehensive education and awareness initiatives in relation to online safety.
Parents/guardians	Monitoring children's online activities and educating themselves about online risks to children.
Private Sector (including online platforms)	Putting in place systems and processes to identify, mitigate and manage the risks of harm, ensuring appropriate mechanisms for transparency, accountability, and user redress. Protecting children's data and privacy online and supporting education and awareness initiatives.

[17] For example: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/readout-of-white-house-task-force-to-address-online-harassment-and-abuse-youth-roundtable/

Research and academia (interdisciplinary)	Interdisciplinary research focusing on empirical field work; data aggregation and analysis; and technological solutions.

To clarify, the table above does not pertain to all roles that stakeholders will play in any given contexts. However, based on research and consultations, the table suggests some general guidance for designing strategies involving multiple stakeholders.

3. PROMOTE GLOBAL COOPERATION TO FURTHER ONLINE CHILD SAFETY

The Indian Presidency's mapping exercise revealed that there are several commonalities in the stakeholders, risks, and responses across G20 members. Countries would benefit from leveraging existing fora such as the Five Country Ministerial (FCM), G7 Child Sexual Exploitation Working Group and the WeProtect Global Alliance Taskforce for information exchange, sharing best practices and collaborations on research to tackle online risks.

4. CRITICAL ROLE OF BUSINESSES AND ONLINE PLATFORMS

Online safety is a systemic issue, and the private sector plays a vital role in ensuring a safe and trusted environment for children and youth. Online platforms should design processes that enhance and promote transparency and accountability in the design, development and operation of their products and services. For example, Microsoft designed the Family Safety Application that promotes healthy digital habits, content filters, and location tracking.[18] Meta has also adopted a three-pronged industry leading approach to child online safety including preventing harm in the first place; making it easier to report harms; and responding swiftly to existing actions.[19]

In addition, online platforms should be actively involved in educational awareness raising and capacity building activities to ensure children and youth are able to interact and behave safely online, for example, by jointly funding, organizing, and participating in such projects with governments, regulators, and civil society.[20]

END OF PART ONE

[18] https://www.microsoft.com/en-in/microsoft-365/family-safety
[19] https://about.meta.com/actions/safety/onlinechildprotection/;https://about.meta.com/actions/safety/onlinechildprotection/
[20] See for example, Meta's resources for parents https://about.meta.com/actions/safety/audiences/childsafety/

PART TWO:
G20 MAPPING OF CYBER EDUCATION AND CYBER AWARENESS INITIATIVES FOR CHILDREN AND YOUTH

INTRODUCTION

This mapping section forms the basis of G20 Toolkit on Cyber Awareness and Cyber Awareness for Children and Youth and must be read as a backgrounder and research supplement to the toolkit. This mapping document contains:

1. A survey of relevant academic and policy literature on the risks faced by the target demographic of children and youth.
2. Policy and regulatory solutions as well as cyber awareness and cyber education measures undertaken by G20 member states along with other stakeholders.
3. The accompanying toolkit analyses the data surveyed, providing a structural premise illustrated through a response pyramid for evaluating the responses to the identified risks, and concludes with policy recommendations that governments can consider when devising intervention strategies to counter cyber risks faced by children and youth.

SURVEY OF SECONDARY LITERATURE

SURVEY OF RISKS

The online safety of children and youth has been studied by a number of academic experts, researchers and institutions from multiple perspectives and disciplines. This section provides an overview of the surveyed secondary literature.

Seminal work has been produced on identifying and classifying the risks faced by children and youth. In 2017, UNICEF built on the EU Kids Online classification of risks to define the 3Cs of online risk: content risks, contact risks, and conduct risks.[21] The classification stems from the source of the category. Content risks cover exposure of children or young adults to inappropriate content; contact risks stem from direct contact or communication with an adult seeking inappropriate behaviour and conduct risks refer to inappropriate behaviour exhibited by children themselves.

In 2021, the OECD undertook a holistic survey of risks faced by children to come up with a new classification that involved an additional 'C': content risks, contact risks, conduct risks, and a fourth risk category labelled 'consumer' risks, which recognized increasing exposure of children and youth to the online financial ecosystem[22]. A summary of the OECD's classification is reproduced in Figure 2.

Risks for Children in the Digital Environment				
Risk Categories	**Content Risks**	**Conduct Risks**	**Contact Risks**	**Consumer Risks**
Cross-cutting Risks*	Privacy Risks (Interpersonal, Institutional & Commercial)			
	Advanced Technology Risks (e.g. AI, IoT, Predictive Analytics, Biometrics)			
	Risks on Health & Wellbeing			
Risk Manifestations	Hateful Content	Hateful Behaviour	Hateful Encounters	Marketing Risks
	Harmful Content	Harmful Behaviour	Harmful Encounters	Commercial Profiling Risks
	Illegal Content	Illegal Behaviour	Illegal Encounters	Financial Risks
	Disinformation	User-generated Problematic Behaviour	Other Problematic Encounters	Security Risks

Figure 2: OECD (2021) Typology of risks

Scholars Livingstone and Stoilova conducted practitioner consultations to verify the usability of their 4C framework for researchers and other stakeholders working in this space. They also reviewed prior classifications of online risks to children by UNICEF, ITU, OECD, Council of Europe, and others to arrive at the CO:RE consortium

[21] UNICEF, State of the world's children: Children in a digital world 2017 www.unicef.org/publications/index_101992.html
[22] OECD, Children in the Digital Environment: Revised Typology of Risks, 2021 https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf?expires=1691492301&id=id&accname=guest&checksum=8D615B30F42A517BF08F9D523D8E04CB

framework for assessing online risks to children.[23] The cross-cutting risks were identified due to the complex and interrelated nature of the digital ecology which meant that harms could impact multiple dimensions of a child's experience. This included the 4Cs framework proposed by the OECD as well as the three cross-cutting risks including:

1. Privacy violations (interpersonal, institutional, commercial).
2. Physical and mental health risks (sedentary lifestyle, isolation, anxiety).
3. Inequalities and discrimination (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics.

UNICEF has been at the forefront of this empirical work and has surveyed children in over thirty countries to arrive at some critically important statistics, such as:

1. More than a third of young people in 30 countries feel exposed to cyber bullying with 1 in 5 not attending school due to this fear.
2. 80% of young people in the 30 surveyed countries were exposed to online sexual abuse or exploitation.

Some useful studies have also done a synthesis through meta-analysis of other empirical work to provide a holistic statistical understanding of the nature and extent of risks faced by children online.[24] One such detailed empirical study concludes that approximately one in five youth were exposed to unwanted sexually explicit material and one in nine youth were faced with online sexual solicitation, thus underlining the need for education campaigns and internet risk strategies. [25]

MAPPING OF G20 MEMBER INITIATIVES

A second bucket of literature provides insights on measures and policy initiatives specifically undertaken by some countries to counter these risks. UNICEF's Disrupting Harms Online was a fourteen-country research project established in partnership with ECPAT International and INTERPOL to generate high-quality evidence on technology-facilitated sexual exploitation and abuse of children.[26] One study by Global Forum on Cyber Expertise has provided rigorous evaluation of the policy landscapes in thirteen countries, i.e., Australia, Canada, Estonia, Greece, Mexico, New Zealand, Norway, Portugal, Singapore, South Africa, The Netherlands, UK and USA.[27] This is followed by some general recommendations for each stakeholder. By adopting a combination of desk research and expert interviews, the report provides a solid evidence base. This mapping section builds on this existing research by surveying all G20 members and building on insights directly received from G20 governments.

GLOBAL GUIDANCE AND RECOMMENDATIONS

A final bucket of surveyed literature proposes solutions. In 2021, the Committee on the Rights of the Child published *General Comment No. 25 on Children's Rights in relation to the Digital Environment* drawing from consultations

[23] Sonia Livingstone and Maria Stoilova, "The 4Cs: Classifying Online Risk to Children" (Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); 2021)https://doi.org/10.21241/ssoar.71817

[24] Sheri Medigan et al, "The Prevalence of unwanted online sexual exposure and solicitation among youth: A meta-analysis" Journal of Adolescent Health Volume 63 No 2 (June 2018) Available at https://www.jahonline.org/article/S1054-139X(18)30134-4/fulltext

[25] Ibid

[26] https://www.unicef-irc.org/research/disrupting-harm/

[27] GFCE, Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people (2022), Available at: https://cybilportal.org/wp-content/uploads/2022/03/GFCE-Research-Report-Pre-University-Cyber-Security-Education_20220210.pdf

with several stakeholders, including children.[28] The General Comment explains how governments can implement the Convention on the Rights of the Child in the digital environment and outlines a range of implementation measures including legislation; comprehensive policy and strategy; coordination; data collection and research; dissemination of information, awareness-raising and training; cooperation with civil society; children's rights with regard to the business sector; among others.

The ITU COP Guidelines for policymakers provide high level recommendations for countries to refer to while drafting and implementing national strategies on Child Online Protection. [29]A report authored by UNICEF provides guidance to countries on how to devise legislation to prevent child sexual abuse online.[30] Another report by Renaud&Prior focuses on interventions targeted towards mitigating risky behaviour by children.[31] The report provides three options (the '3Ms') of mentor, mitigate, and monitor to counter specific examples of risky behaviour. The World Economic Forum (WEF) has also published a detailed white paper listing priority action items for several stakeholders including employers, digital platforms, advertisers, and regulators.[32] This is a useful 'call to action,' and rightfully identifies that the solution lies in building an effective multistakeholder ecosystem.

This toolkit builds on WEF's call to action by identifying more important stakeholders including parents, teachers, and law enforcement. Further, this paper shares a response structure that is targeted towards each specific risk and vulnerability that has been devised, which provides a concrete decision-making action plan for policymakers. Below is a non-exhaustive list of existing international efforts to promote cyber awareness and cyber education for children.

Organisation	Recommendations
End Violence Against Children[33]	1. Integrate digital skills education into both life skills and education programming. 2. Push for child online safety strategies wherever and however possible. 3. Raise awareness about online child sexual exploitation across networks. 4. Invest in the End Violence Fund. 5. Join the Global Partnership to End Violence against children.
WeProtect Global Alliance to eradicate online child sexual abuse- Model	1. Policy, legislation, and governance 2. Criminal justice 3. Victim support and empowerment 4. Society and Culture

[28]Office of the United Nations High Commissioner for Human Rights, General comment No. 25 (2021) on children's rights in relation to the digital environment (2021), Available at: United Nations CRC/C/GC/25

[29] ITU, "Guidelines for policymakers on Child Online Protection", 2020, https://www.itu-cop-guidelines.com/_files/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[30]UNICEF, Legislating for the digital age (2022), Available at: https://www.unicef.org/media/120386/file/Legislating%20for%20the%20digital%20age_Global%20Guide.pdf

[31] Karen Renaud and Suzanne Prior, "The "Three M's" Counter-Measures to Children's Risky Online Behaviours: Mentor, Mitigate and Monitor" (2021), Available at: https://strathprints.strath.ac.uk/75035/6/Renaud_Prior_ICS_2021_counter_measures_to_childrens_risky_online_behaviours.pdf

[32] World Economic Forum, "Advancing Digital Safety: A Framework to Align Global Action" (2021), Available at: https://www3.weforum.org/docs/WEF_Advancing_Digital_Safety_A_Framework_to_Align_Global_Action_2021.pdf

[33]https://www.end-violence.org/sites/default/files/paragraphs/download/Online%20Child%20Safety%20175.pdf

National Response[34]	5. Industry's role 6. Effective research and data gathering
ASEAN (Regional Plan of Action for the Protection of Children from Online)[35]	1. Promote, develop, and implement comprehensive national legal frameworks to improve child protection standards and policies. 2. Enhance law enforcement, judicial and legal professional capabilities through regular, relevant, and updated training and exchange of best practices on protecting children from online exploitation and abuse. 3. Encourage setting up national specialised units mandated to lead, support, and coordinate investigations. 4. Ensure right-based, gender and age-responsive child protection and support services and social programs are efficient. 5. Strengthen data collection and monitoring, reporting and referral mechanisms through hotlines to report harmful content including CSAM. 6. Promote a national education programme and school curricula to raise awareness about children's exploitation among children, youth, parents, guardians, caregivers, practitioners, and community. 7. Engage with the private sector and other stakeholders in monitoring, prevention, and response mechanisms of CSAM through regulations, corporate social responsibilities.
ITU Child Online Protection for Policy-Makers[36]	1. Recommendations on a legal framework. 2. Regulatory framework. 3. Reporting harmful content 4. Reporting user concerns 5. Actors and stakeholders. 6. Research. 7. Education digital literacy and competency. 8. Educational resources. 9. Child protection. 10. National awareness. 11. Tools, services, and settings. 12. Recommendations are based on the following principles: 13. Based on a holistic vision that incorporates government, industry, and society. 14. Result from an all-encompassing understanding and analysis of the overall digital environment yet be tailored to the country's circumstances and priorities. 15. Respect and be consistent with the fundamental rights of children as enshrined in the UN Convention on the Rights of the Child and other key international conventions and laws. 16. Respect and be consistent with existing, similar, and related domestic laws and strategies in place such as child abuse laws or

[34] WeProtect Global Alliance to eradicate online child sexual abuse- *A Model National Response* & *Model National Response Maturity Model* (2022). Available at: https://www.weprotect.org/model-national-response/

[35] https://asean.org/wp-content/uploads/2021/11/4.-ASEAN-RPA-on-COEA_Final.pdf

[36] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.POL_MAKERS-2020-PDF-E.pdf

	child safety strategies. 17. Respect children's civil rights and freedoms, which should not be sacrificed to protection. 18. Developed with the active participation of all relevant stakeholders including children, addressing their needs and responsibilities, and meeting the needs of minority and marginalized groups. 19. Designed to align with broader government plans for economic and social prosperity and maximize the contribution of ICTs to sustainable development and social inclusion. 20. Utilize the most appropriate policy instruments available to realize its objective, considering the country's specific circumstances. 21. Set at the highest level of government, which will be responsible for assigning relevant roles and responsibilities and allocating sufficient human and financial resources. 22. Help build a digital environment that children, parents/caregivers, and stakeholders can trust. 23. Guide efforts of stakeholders to empower and educate children on digital literacy to protect themselves online.
OECD Recommendations[37]	1. Demonstrate leadership and commitment considering the best interests of the child in the digital environment. 2. Review, develop, and amend as appropriate, laws that directly or indirectly affect children in the digital environment. 3. Promote digital literacy as an essential tool for meeting the needs of children in the digital environment. 4. Adopt evidence-based policies to support children in the digital environment. 5. Promote the adoption of measures that provide for age-appropriate child safety by design. 6. Promoting international cooperation among international and regional networks through measures such as developing shared standards.
OHCHR General Comment No. 25	1. It identifies four principles to guide measures on protection of children's rights, namely - non-discrimination, best interests of the child, right to life, survival and development and respect for the views of the child. 2. States should respect the evolving capacities of children. 3. Opportunities to realise children's rights and their protection need to be created through legislative, administrative, and other measures. 4. Children should have rights such as access to information in the digital environment, freedom of expression, privacy, among others. 5. States should take measures to protect children from violence in the form of participation in online child sexual abuse, cyberaggression, among others. 6. Parents and caregivers need to be sensitised on how to balance child's protection and supporting their autonomy.

[37] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389#mainText

	7. It is important to promote technological innovations for children with different types of disabilities.
5 Rights Handbook[38]	Enablers include: 1. Cross-sector, multidisciplinary collaboration. 2. Willingness to prosecute, functioning justice system and the rule of law. 3. Supportive reporting environment. 4. Aware and supportive public and professionals, working with and for children. 5. Sufficient financial and human resources. 6. National legal and policy frameworks in accordance with the UNCRC and other international and regional standards. 7. Data and evidence in child sexual abuse.

Table 2: Summary of (non-exhaustive) policy guidance

[38] https://www.weprotect.org/wp-content/plugins/pdfjs-viewer-shortcode/pdfjs/web/viewer.php?file=https://www.weprotect.org/wp-content/uploads/MNR-DV2.pdf&attachment_id=238075&dButton=true&pButton=true&oButton=false&sButton=true#zoom=0&pagemode=none&_wpnonce=b8a4334dff

NATURE OR RISKS FACED BY CHILDREN & YOUTH

This section provides a specific description of each risk faced by children and youth based on a curated analysis of publicly available documents released by G20 members and inputs gathered through a circulated questionnaire. The classification of risks draws from OECD's 2021 risk classification framework.

CONTENT

Content risks refer to situations "where a child or young adult is exposed to unwelcome and inappropriate content." Inappropriate content may be targeted towards the consumer or be mass produced.[39]

Misinformation and disinformation

Misinformation is false or misleading information that is unwittingly shared whereas disinformation is deliberately created with an intent to deceive or harm. Children are frequent users of the internet and use social media regularly. A 2020 study estimates that 76 percent of 14–24-year-olds reported seeing online mis/disinformation once a week. UNICEF has shown that children may fall prey to mis/disinformation due to their evolving cognitive and psychological capacities.[40]

Hateful Content

Cyber hate often refers to online hate speech that is expressed digitally through devices like computers and mobile phones. Hate speech attempts to spread and justify intolerance and discrimination based on ethnicity, religion, sexuality, and other factors. Findings from a report by EU Kids show that encountering cyberhate content on the internet is quite prevalent among children aged 11-17 years. This varies across the countries surveyed though: 21 percent of children in France reported that they had been exposed to some form of hateful content online whereas the same applied for 59% of Czech children.[41] Exposure to online hate can significantly harm the self-esteem and mental well-being of children, especially from vulnerable communities.[42] We note that countries have different standards and definitions for hateful content.

Other harmful content

Exposure to other harmful content such as online pornography can significantly harm children and lead to poor mental health, sexism, and objectification. This threat should be differentiated from the contact threat of producing and dissemination of Child Sexual Abuse Material online. Research has also shown that exposure to pornography as a child or youth may influence life satisfaction, sexual behaviour and pornography viewing patterns in adulthood.[43]

CONSUMER

Consumer risks are risks faced by children and youth owing to their participation as consumers in and use of the financial facets of the digital environments. These are often perpetrated through[44] the use of social methods of

---

[39] Sonia Livingstone and Maria Stoilova, the 4Cs: Classifying Online Risk to Children. (Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); 2021) https://doi.org/10.21241/ssoar.71817

[40]UNICEF, Digital misinformation/disinformation and children (2021), Available at: ttps://www.unicef.org/globalinsight/media/2096/file/UNICEF-Global-Insight-Digital-Mis-Disinformation-and-Children-2021.pdf

[41] MUNI, Children's experiences with cyberhate - new research report (2020), Available at: https://irtis.muni.cz/news/childrens-experiences-with-cyberhate-report

[42] Sue Jones, "What is the real-world impact of online hate speech on young people?" Available at: https://www.internetmatters.org/hub/question/what-is-the-real-world-impact-of-online-hate-speech-on-young-people

[43] Bonnie Young, "The Impact of Timing of Pornography Exposure on Mental Health, Life Satisfaction, and Sexual Behavior" (2017) Available at; https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=7727&context=etd

[44] Turkiye response to circulated questionnaire.

manipulation to which children and youth are particularly susceptible that could force individuals to divulge information or engage in risky behaviour online.

Fraud

Online financial scams and frauds may target individuals of any age, however, children and youth can be considered to be more vulnerable.

Profiling

Commercial profiling, where personal data is used to create marketable digital profiles for advertising or other commercial purposes, poses risk for all users that may be exacerbated in the absence of informed consent and may in some cases violate applicable consumer and/or data protection laws. If they do not have adequate digital literacy skills, then children may be specifically susceptible to profiling risks through interactions in the digital environment.

Data Privacy and Security

Data privacy and security are specific risks to children as they may limited of understanding of how their data is processed and inferred. In some countries, the risks may be mitigated by requirements that parents consent to information collection about children. Research suggests that data privacy must be understood at two levels: interpersonal privacy that concerns the direct relationship between the child and the entity that it provides the data to as well as institutional and commercial privacy that deals with how that data is processed and inferred.[45] It found that there are significant differences in the understanding of both these facets of privacy among 5–7-year-olds, 8–11-year-olds and 11- to 17-year-olds.[46] This is a particular challenge for data classified as sensitive such as health data and biometric information.

CONDUCT

Conduct risks occur when a child witnesses, participates in or is a victim of potentially harmful conduct by other children or adults online.

Internet addiction and over-use

All over the world, children are spending increasing amounts of time on the internet, causing parents and caregivers to fear that they are missing out on real world experiences. There are other risks too such as physical health risks, mental distress, and insomnia.[47] Estimates suggest that children and youth of ages from 8 to 28 years spend about 44.5 hours each week on digital devices.[48] Video games pose a specific risk on this front as about 23% of children have reported that they feel addicted to video games.[49]

Cyberbullying

Cyberbullying is bullying using digital technologies such as social media platforms, messaging or chat platforms

---

[45] Mariya Stoilova et al, "Children's data and privacy online" (2019) London School of Economics, Available at: https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

[46] Mariya Stoilova et al, "Children's data and privacy online" (2019) London School of Economics, Available at: https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

[47] Tyler Clark, Internet Addiction - How much is too much time on the internet?" Available at: https://centerforparentingeducation.org/library-of-articles/kids-and-technology/how-much-time-internet-kids

[48] Ibid

[49] Ibid

and gaming sites.[50] All G20 countries recognize cyberbullying as a key risk. Italy has an explicit law on cyberbullying that defines it as "whatever form of psychological pressure, aggression, harassment, blackmail, injury, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, unlawful processing of personal data of minors and/or dissemination made through electronic means, including the distribution of online content depicting also one or more components of the minor's family whose intentional and predominant purpose is to isolate a minor or a group of minors by putting into effect a serious abuse, a malicious attack or a widespread and organized ridicule".[51] Cyberbullying includes hateful encounters based on the racial, ethnic, religious or gender identity of the child or youth. Cyberbullying could be classified as a conduct or a contact risk depending on whether it is carried out by a child or by an adult.

Intimate image abuse

Intimate image-based abuse takes place when an individual leaks or threatens to leak an intimate image of a child or youth. Sometimes the images are manipulated and with the increasing use of digital technologies, intimate image abuse has increased significantly.[52] Depending on the nature of the image, intimate image abuse could also be classified as distributing child sexual abuse material.

CONTACT

Content risks are defined as risks that the "child experiences or is targeted by contact in a potentially harmful adult-initiated interaction, and the adult may be known to the child or not."

Cyber Grooming

The International Labour Organisation, in the Terminology Guidelines for the Protection of Children from Online Exploitation and Abuse ("Luxembourg Guidelines") defines grooming as a "process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person".[53] According to the National Commission for Protection of Children's Rights in India, online grooming describes tactics including bribes, flattery, sexualised games, desensitization, risks and blackmail to build an emotional connection with the child such that they do not understand that they are being groomed.[54] Grooming could be utilised as the first step towards exploiting the child to produce sexual abuse material.

Child sexual abuse material (CSAM)

The Convention on the Rights of the Child requires State Parties to take all appropriate measure to prevent "the exploitative use of children in pornographic performances and material."[55] The Optional Protocol to the Convention on the Rights of the Child on the sale of Children, Child Prostitution and Child Pornography[56] defines

[50] UNICEF, Cyberbullying: What is it and how to stop it" Available at: https://www.unicef.org/end-violence/how-to-stop-cyberbullying.
[51] Italy, Provisions on cyberbullying and stalking, Available at: https://www.coe.int/en/web/cyberviolence/italy
[52] Clare McGlynn, Erika Rackley, and Ruth Houghton Beyond 'Revenge Porn': The continuum of image-based sexual abuse. Feminist Legal Studies, 25 no 2 (2017) 25-46.
[53] International Labour Organisation, *Terminology Guidelines for the protection of children from sexual exploitation and sexual abuse*.2016. https://www.ilo.org/ipec/Informationresources/WCMS_490167/lang--en/index.htm
[54]National Commission for Protection of Child Rights, *Being safe online: Guideline for raising awareness among children, parents, educators, and general public* .2017. https://www.childlineindia.org/pdf/Being-Safe-Online-Guideline-and-standard-content-for-raising-awareness-among-children-parentseducators-and-general-public.pdf
[55] UN Convention on the Rights of the Child https://www.unicef.org/child-rights-convention/convention-text
[56] Available at https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child

child pornography as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes." Additionally, Article 3(c) of the Optional Protocol calls upon states to use domestic legislation to criminalise "[p]roducing, distributing, disseminating, importing, exporting, offering, selling, or possessing child pornography."

State Parties have largely complied with this provision in the Optional Protocol and all G20 members have criminalized CSAM. The legal definition of child pornography is complex and varies across jurisdictions based on the range of offenses that the criminal legislation in question endeavours to tackle. While 'child pornography' continues to be a term used in case law and statute, there is a case for using other terms for more precise policy understanding. Recently, reports by NGOs[57]and international law enforcement authorities[58] have acknowledged the importance of the term "child sexual abuse material" which can be used to cover images or media depicting sexual abuse or sexual acts for minors who cannot consent. The term "child sexual exploitation material" covers all other sexualised material depicting children.[59]

Despite this widespread recognition, statistics on the rise of child sexual abuse material are disturbing. A report by the Internet Watch Foundation flagged 150,000 web pages globally as having child sexual abuse material.[60] This marked a 77% rise in the proportion of websites containing child sexual abuse material since 2016. The US-based National Centre for Missing and Exploited Children's (NCMEC) cybertipline in 2022 received more than 32 million reports of suspected child sexual exploitation. Over 99.5% of those reports related incidents of possible child sexual abuse material (31,901,234). Internet Service providers submitted 49.4 million pieces of child sexual abuse material 18.8 million (38%) were unique- never seen before. This is indicated by new and possibly ongoing abuse.[61]

Online Sexual Encounters

Children could face a range of other online sexual encounters that are not initiated for the purpose of creating child sexual abuse material. These include sexually expletive or abusive texts shared through messaging platforms or mobile based messaging services ('sexting').

[57] Child Rescue Coalition, "It's not child pornography, it's child sexual abuse material," https://childrescuecoalition.org/educations/its-not-child-pornography-its-child-sexual-abuse-material

[58] Guideline prepared by Interpol available at: https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology

[59]International Labour Organisation, *Terminology Guidelines for the protection of children from sexual exploitation and sexual abuse*. 2016. https://www.ilo.org/ipec/Informationresources/WCMS_490167/lang--en/index.htm and https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---ipec/documents/instructionalmaterial/wcms_490167.pdf pp.40

[60] Internet Watch Foundation, Child sexual abuse imagery reports. 2020. https://annualreport2020.iwf.org.uk/trends/international/overview

[61] Shared by the European Union for this suggestion. Data available here https://www.missingkids.org/cybertiplinedata

POLICY RESPONSES

G20 countries have recognized the aforementioned risks and adopted a range of policy interventions, including regulatory measures and cyber education and cyber awareness initiatives.

LEGISLATION AND REGULATORY SOLUTIONS

Legislation and regulatory solutions refer to top-down legal obligations imposed by the government with civil or criminal sanctions for non-compliance.

For contact risks, G20 members have adopted a range of criminal legislation, especially to counter and criminalize CSAM (more appropriately referred to as 'child sexual abuse material.') These criminal provisions are either included in the omnibus criminal legislation or legislation specific to the protection of children. For example:

- Argentina: Article 128 of the Penal Code imposes criminal liability on anyone who "produces, finances, offers, trades, publishes, facilitates, discloses or distributes by any means, any representation of a minor under eighteen dedicated to explicit sexual activities or any representation of their genital parts for predominantly sexual purposes." Argentina also punishes possession to and facilitation of access to pornographic material.

- Türkiye: Article 226 of The Turkish Criminal Code Law No. 5237, criminalizes producing, distributing, copying, selling, transporting, storing, exporting, and possessing obscene written or audio-visual materials using children. The Code also punishes giving, reading, inducing another to read, making watch or listen to such materials to children.[62]

- Germany: The German Criminal Code prohibits the distribution, acquisition and possession of pornography involving children (under 14 years of age) and juveniles (between 14 and 18 years), respectively. These sections involving all children and all juveniles semantically (involving all children) pertain to "written materials," and the definition of written materials also encompasses audiovisual media, data storage media, illustrations, and other depictions. The Criminal Code also punishes realistic portrayals of sexual abuse material such as virtual pornography.

- India: India's Protection of Children from Sexual Offences (POCSO) Act criminalizes "use (of) a child or children for pornographic purposes," and the punishment includes at least five years imprisonment with fine. In case of a second conviction, the punishment can be extended to seven years of imprisonment along with a fine. Section 15 of the Act also prohibits storing or possessing CSAM.

Several countries separately criminalize grooming and other contact risks related to sexual exploitation. For example:

- Mexico: Mexico's Federal Penal Code Article 202 punishes the production, possession, distribution, selling, purchase, lease, exhibition, publication, transmission, importation, or exportation of CSAM for commercial

[62] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)011-e

purposes and includes criminal sentences for 7 to 12 years. It also penalizes grooming or soliciting children for the purpose of participating in pornographic performances.

- Türkiye: Türkiye's Criminal Code Law No. 5237 Article 103 criminalizes and punishes all kinds of sexual attempt against children who are under the age of fifteen or against those attained the age of fifteen but lack the ability to understand the legal consequences of such act and sexual behaviours committed against other children by force, threat, fraud, or another reason affecting the willpower. Article 104 punishes any person who has sexual intercourse with a child who completed the age of fifteen, without using force upon filing of a complaint.

- European Union: The Council of Europe in Article 23 of Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse criminalizes grooming that has been committed "through the use of information and communication technologies." The provision specifies that the initial overture must be followed by a proposal to meet the child in person with the purpose to engage in sexual activities with a child or to produce CSAM, and by material acts leading to such meeting.

- Saudi Arabia: In Saudi Arabia, Article 8, Clause 3 of the Anti-Cybercrimes Law defines "the luring and exploiting of minors" as an aggravating circumstance for the listed violations, resulting in the imprisonment and fine being not less than half the maximum. The Anti-Harassment Act, Article 6 states that the involvement of a child represents an aggravating circumstance for any of the previously mentioned crimes.

- India: India does not specifically outlaw grooming, but a number of legal provisions can be used to hold perpetrators accountable. Section 11 of the POCSO Act deals with the sexual harassment of children, which includes any of the following accompanied by sexual intent such as communication with the child, showing a part of the body to the child, making the child exhibit their body, showing any media for pornographic purpose, stalking the child, threatening to use a real or fabricated depiction of the means constitutes sexual harassment, which may be applied to instances concerning online grooming of children.

Cyberbullying has also been criminalized by some countries regardless of whether the perpetrator is a minor or an adult.[63] As shared above, Italy has passed specific legislation to tackle cyberbullying and has specifically defined cyber bullying, as discussed above in the definition section. The legislation takes a broad view of cyberbullying and also provides victims of cyberbullying the right to have the flagged content removed within 48 hours.

Under Australia's Online Safety Act 2021[64], the eSafety Commissioner administers regulatory and reporting schemes, including Cyberbullying (children) Cyber Abuse (adults), Image-based Abuse, and Illegal and Restricted Content (including child sexual exploitation material). Under these schemes, individuals can report harmful content to eSafety. If a complaint meets the regulatory threshold, eSafety has the authority to require technology platforms to remove seriously harmful content within 24 hours and can impose civil penalties on

[63] For example, see Ireland's Coco's law, Harassment, Harmful Communications and Related Offences Act 2020
[64] Input received from the Australian delegation

technology platforms who fail to comply.[65]

In terms of content risks, G20 countries have passed general legislation imposing obligations on social media intermediaries to moderate content including disinformation and hate speech. Such legislation has largely not been targeted towards children or youth as the consumers, so far. For example:

- Germany's response[66] to the circulated questionnaire provided information on German legislation tackling hateful content:

  The publication of severely hateful content within Germany is (in addition to being actionable under criminal law) illegal according to the Youth Protection Act (JuSchG) as well as the Interstate Treaty on the protection of minors (JMStV). The publication of such content can be prosecuted by law enforcement. Content that is severely hateful but does not cross the threshold into illegality may be included in the List of Media Harmful to Young Persons, data and telemedia which are then subject to extensive sales and distribution restrictions as well as an advertising ban.

  Within Germany various institutions work on media education, providing information as well as recommendations on dealing with hateful content. In Germany, the Network Enforcement Act (NetzDG) obliges social networks with more than 2 million users in Germany to delete or to block access to certain unlawful content within a short period of time after they have become aware of it through a user complaint. Unlawful content is any content that fulfils one of the criminal offenses listed in 1 NetzDG. This may include hateful content. Violations of the provisions of the NetzDG can be punished with a fine of up to EUR 50 million. The DSA sets out uniform and directly applicable requirements for online platforms throughout the EU for the moderation of online content, in particular for a reporting and remediation procedure for illegal content.

- Japan's response to the circulated questionnaire stressed on the need to focus on business entities related to internet use by young people:

  The Law and the Basic Plan state as one of its basic principles to promote various measures to improve the performance and disseminating the use of software for filtering content harmful to young people and the business entities engaged in businesses related to internet use by young people shall endeavor, by the characteristics of their businesses, to take measures to reduce the chances of young people viewing harmful content via the internet as much as possible.

- Türkiye's response to the circulated questionnaire suggested that they were working with multiple stakeholders to implement its legislation:

  In Türkiye, the Information and Communication Technologies Authority is working in collaboration with internet actors and stakeholders to combat illegal and harmful online content. This effort is being carried out

[65] See resources at: For educators and schools | eSafety Commissioner

[66] As per inputs from Germany "Cybermobbing"and "cyberbullying" do not exist as separate offenses in the German Penal Code (StGB). The provisions of the German penal code which define the punishable offences, apply to all persons who have reached the age of 14. The Youth Courts Act (JGG) applies to juveniles (14 to 17 years of age) and young adults (18 to 20 years of age); it does not provide for amendments of offences but especially for particular regulations concerning the criminal proceedings and the sanctions and measures applicable to young offenders."

under the Law No. 5651, which regulates internet publications and aims to prevent crimes committed using such publications.

For consumer risks, countries have adopted specific provisions in their legislations that are designed to protect children. These provisions are usually found in general consumer protection or data protection legislation, although some jurisdictions have carved out specific legislation for protecting children's privacy. One method has been to mandate parental consent below a certain age, such as 13 years for certain content in the case of Children's Online Privacy Protection Act in the United States and 16 years in the case of the General Data Protection Regulation (GDPR) in the European Union. China has also passed legislation titled Provisions on Cyber Protection of Personal Information of Children that specifically deals with data protection concerns when it comes to children.

A few countries have passed regulations or guidelines on online advertising for children. Most of these guidelines are contained in the national self-regulatory advertising codes. For example:

- Brazil: Article 37 of the Brazilian Code of Advertising Self-Regulation makes it illegal to associate children with illegal, dangerous, or socially reprehensible situations. Children are also forbidden from featuring in advertisements that promote inappropriate products such as armaments or alcohol.

- Türkiye: Article 61/3 of Türkiye's Law on Consumer Protection No. 6502 does not allow commercial advertisements that deceive or mislead the consumer, or abuse the consumer's lack of experience or knowledge, threatening the life of the consumer and safety of his property, encouraging the acts of violence, or inciting to commit crime, endangering public health, abusing the sick, elderly, children, or disabled people.[67]

- India: Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements states that "An advertisement of any goods, product or service that addresses or targets children shall not – (a) be such as to develop negative body image in children; (b) give any impression that such goods, products or services are better than the natural or traditional food that children may be consuming."

- Indonesia: The self-regulatory guidelines titled Indonesian Advertising Code of Ethics prevents alcohol advertisements to individuals below the age of 21 years and tobacco advertisements to those below 18 years.

Conduct risks have safeguarding legislation from few members in the G20, other measures such as education and awareness appear to be more appropriate. In terms of access and grievance redressal, various institutions of governments have contributed either individually or in collaboration with other governmental institutions through an 'all of government' approach. Law enforcement institutions have set up helplines that can easily be reached by victims of cyber risks, especially child sexual exploitation.

[67] https://ticaret.gov.tr/data/5d42a9b313b87632542a2dae/LAW%20ON%20CONSUMER%20PROTECTION.pdf

CYBER EDUCATION INITIATIVES

Some G20 countries have provided centralized guidelines that all schools must follow when imparting courses related to cybersecurity. Some schools, along with relevant experts from civil society and other stakeholder groups, have formulated online course material that can be used by parents and students to further equip themselves on cyber education. For example:

- In the United Kingdom, all schools are required to teach students about online safety. There is a national curriculum that must be followed by local authority schools. [68]

- In Germany, the Strategy "Education in the Digital World" (2016) of the Standing Conference of Ministers of Education and Cultural Affairs of the Länder identifies the ability to act safely in digital environments as one of the core digital competencies.

- Australia's eSafety Commissioner has produced a range of education materials to support schools in the delivery of online safety education, including the development of best practice guidance and implementation tools (the Best Practice Framework for Online Safety Education and Toolkit for Schools), and materials for educators and parents that are aligned with the Australian curriculum.[69]

- According to the European Union's response to the circulated questionnaire, the European Commission has undertaken a coordinated effort and invested funding to ensure cyber education that reaches the most vulnerable population:

  "Education and training are fundamental in developing digital literacy and citizenship from early on and in a continuous manner. With the Digital Education Action Plan, our goal is to ensure that young people have the digital skills and competences needed for the digital society, including digital literacy, critical thinking, and engagement with information online. In October 2022, the Commission published hands-on Guidelines for teachers and educators to promote digital literacy and tackle disinformation in the classroom, in a direct response to these pressing societal issues. The guidelines are translated into all EU official languages so that all teachers and learners can benefit from them straight away. In addition, Erasmus+ as a main funding programme in education has been providing valuable support for grass-root projects in the field for years - in 2021, 90 new projects dealing with media literacy and disinformation were awarded funding. Going further, the Forward-Looking Call in 2023 looks specifically for projects promoting teacher training and curriculum development on the topic. Lastly, the eTwinning community dedicated its annual theme in 2021 on 'Media Literacy and fighting Disinformation', which resulted in different events and a book with good teaching practices."

- In Türkiye, there is a strong dedication to multiple elements of education programs. While cybersecurity training camps, vocational high schools, and junior technical colleges with expertise in cybersecurity provide cybersecurity education for youth, the Information and Communication Technologies Authority Academy as

[68] Department for Business, Innovation Skills, "School children as young as 11 to get cyber security lessons,"*Gov.UK*,March 13,2014, https://www.gov.uk/government/news/school-children-as-young-as-11-to-get-cyber-security-lessons
[69] See resources at: For educators and schools | eSafety Commissioner

a virtual portal provides open and public access to training programs, including cybersecurity. Contests on cyber intelligence and cyber security applied skills promote the awareness and identify the existing and possible qualified workforce in this area.

- In Singapore, the Ministry of Education (MOE)'s Character and Citizenship Education (CCE) curriculum was refreshed in 2021, to have a stronger focus on Cyber Wellness Education. Students learn to be safe, respectful, and responsible users of cyber space, and are taught to seek help from parents and trusted adults should they require support. [70]

- In the USA, NICE, a program of the National Institute of Standards and Technology, coordinates a community that develops guidance for instructors imparting cybersecurity into education at all levels and mechanisms for assessing progress. However, NICE content is targeted at students who want to take up cybersecurity careers rather than to provide general cybersecurity awareness.

    - The U.S. National Summit on K-12 School Safety and Security, hosted by the Cybersecurity and Infrastructure Security Agency (CISA), brings federal, state, and local school leaders together to share actionable recommendations that enhance safe and supportive learning environments in kindergarten through grade 12 (K-12) schools. In January 2023, CISA released the "Partnering to Safeguard K-12 Organizations from Cybersecurity Threats" report and toolkit for K-12 institutions to help them better protect against cybersecurity threats. The report provides recommendations and resources to help K-12 schools and school districts address systemic cybersecurity risk. It also provides insight into the current threat landscape specific to the K-12 community and offers simple steps school leaders can take to strengthen their cybersecurity efforts.

    - The report's findings highlight the importance of resources, simplicity, and prioritization to effectively reduce cybersecurity risk. To address these issues, CISA provides three recommendations in the report to help K-12 leaders build, operate, and maintain resilient cybersecurity programs: invest in the most impactful security measures and build toward a mature cybersecurity plan; recognize and actively address resource constraints; and focus on

- In India, the University Grants Commission has mandated a course on cybersecurity at the university level. This course is stipulated not only for students who want to work on cybersecurity as a profession but for those in other vocations who also need the knowledge to keep themselves and their organizations secure. The course contains a range of modules from the cyber security risk landscape; remedial and mitigation measures; reporting cybercrime as well as advanced topics such as cybersecurity plans and crisis management. The detailed syllabus is available online and can be replicated across jurisdictions.[71]

CYBER AWARENESS INITIATIVES

Most G20 countries have adopted a range of cyber awareness measures targeting an entire ecosystem of stakeholders including the private sector, law enforcement authorities, parents, teachers, and students. While cyber awareness programs must be targeted towards specific demographics, larger societal structures,

[70] Singapore response to circulated questionnaire
[71] Syllabus of cyber security awareness course at undergraduate and postgraduate level. https://www.ugc.gov.in/pdfnews/5457035_Cyber-Security-Final.pdf

processes and tackling systemic issues can certainly enable and augment the ecosystem around child safety.

- As the EU highlights in its response to the circulated questionnaire:

"Development of social and emotional skills, digital skills, and bolstering resilience in children are important to ensure online inclusion. However, other systemic issues such as poverty and inequalities as well as discrimination against children with ethnic or cultural minority backgrounds makes children more vulnerable to negative online experiences such as cyberbullying and grooming."

Indeed, as further indicated in comments by the EU delegation, the "*European strategy for a better internet for kids (BIK+)*[72] *Its first (of three) pillars stands for a safe digital experience to protect children from harmful and illegal online content, conduct, contact and consumer risks and to improve their well-being online through a safe, age-appropriate digital environment, created in a way that respects children's best interests. The BIK+ strategy also specifically focuses on children in vulnerable situations via the activities of the Safer Internet Centres*."

- In France, the laboratory for Childhood Protection Online Charter is a multistakeholder effort modelled on the Christchurch call with a Steering Committee, Executive Committee, Scientific Committee, and Ethical Committee.[73] The Lab was recently launched and will forge a new alliance between regulators, NGOs, digital platforms and academia to identify, implement and independently evaluate technical solutions that will allow us to move forward much faster and, above all, in a more coordinated way in the essential fight to protect children online. The Lab provides an open, empirically based space for conversation. It pursues the dual objective of limiting the risks that digital technology poses to younger audiences while preserving fundamental freedoms in this space. Its members come from the academic world, platforms, civil society, and governments and are organized in the form of committees in charge of one aspect of its operation, the launch of experiments on given issues, and the transparent evaluation of the effectiveness of the tools developed.
- Each year, it selects 3 or 4 projects that its members support in their development by providing adequate resources. The results are shared publicly at the end of the cycle. For the first year of operation, 3 areas of work were selected as part of experimentation tracks: Age verification (by trusted third party; by estimations based on biometric elements), fight against non-consensual sharing of intimate pictures (by the constitution of a shared database of images to be removed), fight against cyberbullying (by the implementation of a network of mediators).
- The laboratory is currently made up of: Estonia, Argentina, New Zealand, academic centres (Berkman Klein Center, Oxford Internet Institute), tech companies (Amazon, Dailymotion, Google, Microsoft, Meta, Niantic, Qwant, Snap, TikTok, Yubo) and civil society associations (Chameleon, e-enfance, Fondation pour l'Enfance, Génération numérique, Internet Sans Crainte, Point de Contact, OPEN, Respect Zone, Safer Internet France, Save the children, Unaf, WeProtect).

[72] https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids

[73] Laboratory for Childhood Protection and Online Charter. https://www.elysee.fr/en/emmanuel-macron/2022/11/10/laboratory-for-childhood-protection-online-charter

- The Scientific Committee can invite experts from academia and other relevant fields such as education, health, social workers, and law enforcement. The goal is to create and share evidence-based research and tools among the participating stakeholders.

Türkiye has taken specific multistakeholder initiatives to combat internet addiction. In its response to the questionnaire, they stated that:

> *"The Safer Internet Center in Türkiye is committed to promoting awareness about internet addiction. The center provides valuable information on internet safety, emphasizing the importance of conscious, safe, and effective use of the internet through its websites, training sessions, and seminars. In addition to these activities, the center also prepares and distributes posters and brochures on the subject. It collaborates with NGOs, public and private entities in the sector to encourage and coordinate similar studies aimed at promoting responsible internet usage."*

The United Kingdom also highlighted several practices it has undertaken in its response to the questionnaire. These include awareness initiatives directed at businesses. It states:

> *"In 2021, the UK published principles of safer online platform design[74] to assist platforms in adopting a safety-by-design approach. Safety by design is the process of designing online platforms to reduce the risk of harm to those who use them. Safety by design is preventative and considers user safety throughout the development of a service, rather than in response to harms that have occurred. The Government has also created a guide for businesses for protecting children online, which summaries key measures[75]."*

Saudi Arabia has shared its cyber awareness practices as well, which include:

"Saudi Arabia launched 'Aamn', a National Cybersecurity Awareness Program and is working on integrating cyber safety courses in school curricula, launching cybersecurity games, and developing awareness campaigns targeting parents and teachers. At the global level Saudi Arabia has recently established Global Cybersecurity Forum Institute, a global platform that seeks to strengthen society's cyber resilience through shared priorities, purposeful dialogue, and impactful initiatives. The National Cybersecurity Agency (NCA) launched a global program on "Creating a Safe and Prosperous Cyberspace for Children", to foster innovative policies, ensure upgrading of skills, promote global dialogue and strengthen global efforts to implement the Child Online Protection (COP) Guidelines."

Through the e-safety commissioner, Australia has also undertaken mass awareness campaigns on online safety, including by designating a Safer Internet Day.[76] The guide for businesses includes measures on data protection and privacy, age-appropriate content, positive user interaction and protection from sexual exploitation. Further, to enable multistakeholder collaboration and to ensure that the government works in

[74] Principles of safer online platform design. June 29,2021. https://www.gov.uk/guidance/principles-of-safer-online-platform-design

[75] Department for Science, Innovation and Technology, A business guide for protecting children on your online platform.29 June 2021. https://www.gov.uk/government/collections/a-business-guide-for-protecting-children-on-your-online-platform.

[76] "Ensuring that cyber safety is front-of-mind for young people, vulnerable groups and seniors is supported in Australia by our first-in-the-world eSafety Commissioner. This includes direct outreach in schools and public communications, including initiatives such as Safer Internet Day. Similar initiatives dedicated exclusively to ensuring that cyberspace is safe for, and can be navigated safely by, young people, can support fostering safer online spaces within and across G20 member nations."

conjunction with the technology sector, there is also dedicated funding for the Safety Tech Innovation Network, an international network dedicated to the promotion, collaboration, and the industrial application of online safety technologies.[77]

Canada has published a range of online resources targeted separately at children, parents, and youth.[78]

As per the response to the questionnaire by Indonesia, decision makers should:

Encourage parents and teachers to advise their children about:

a. *The importance of maintaining privacy in cyberspace, for example what can and cannot be shared*
b. *To be careful with people you don't know, even if they claim to be relatives or over gifts/money/or other treats, children should notify your parents if someone suspicious contacts you*
c. *Do not make any purchase transactions without the knowledge and supervision of parents*
d. *Be careful when you get a link sent in a message, don't click right away, but consult your parents first*
e. *tolerance and ethics in interacting in cyberspace*

International organizations like UNICEF and ITU have been active participants in devising awareness programs. For example:

- Brazil's Internet Segura website has a range of cyber education and cyber awareness materials targeted separately at children, teens, parents and educators, individuals who are 60+, technicians and for general interest.[79]
- ITU has partnered with Italian energy company ENISPA and global accountancy Deloitte to create "Online Safety with Sango [a popular character]" to create an online training course for children[80]

Various institutions of governments have also contributed either individually or in collaboration with other governmental institutions through an 'all of government' approach. Law enforcement institutions have set up helplines that can easily be reached by victims of cyber risks, especially child sexual exploitation. Further, children and youth are not the only ones who it is important to note that several countries have conducted general capacity building programs for instructors, trainers and law enforcement officials who are responsible for nurturing a positive online ecosystem for children and youth.[81]

[77] Website available at https://www.safetytechnetwork.org.uk/
[78] https://www.canada.ca/en/public-health/services/health-promotion/stop-family-violence/resources-keep-children-safe-online.html
[79] https://internetsegura.br/
[80] ITU," Protecting children online: Internet safety with sango" 5 Jul 2021, https://www.itu.int/hub/2021/07/protecting-children-online-internet-safety-with-sango/
[81] Details are provided in the UK's response to the circulated questionnaire.

ANNEX: CIRCULATED QUESTIONNAIRE

Risks

1.What are the major risks faced by children and younger adults in cyberspace?

2.Please provide specific feedback on each of the following risks as outlined in the table below:

Risk/risk category	Specific risk	How does the risk manifest?	What mitigation measures have you taken?
Content	Disinformation		
	Hateful Content		
	Illegal content		
	Others		
Consumer	Fraud		
	Profiling		
	Other financial security risks		
	Data Protection		
	Others		
Conduct	Internet addiction and over-use		
	Cyber-bullying		
	Child sexual abuse		
	Intimate image manipulation		
	Others		
Contact	Grooming		
	Hateful encounters		
	Online sexual violence		

	Others		

3. Out of these risks, do you think that one kind of risk/risk is more dangerous and needs more urgent action than others?

4. Do you have information that you can share with us on the specific risks faced by the following age groups? Please provide information in the following table.

GROUP	Specific threats
Primary school students aged 5-12	
Middle and high school students aged 12-18	
College students aged 18-21	

National Policy and Legislation

5. In terms of national policy, do you differentiate between minor age groups, including by:

(a) Identifying different risks faced by them,

(b) Differentiating between the risks faced by primary school students (5-12) and middle and high school (12-18)

6. Do college students (18-21 years) need to be looked at as a separate group?

7. What risks posed to children and youth can be legislated against? To what extent do you think non-legislative or judicial measures, such as awareness building, and education can be successful in mitigating these risks?

Stakeholders

8. How have you managed to include other stakeholders in the effort to protect children and younger adults from online risks?

Stakeholder	Have you engaged?	How?
Law enforcement		
Educational institutions (schools, colleges)		
Parents		
Teachers		

8. What obligations (legal or self-regulatory) should there be on platforms and other private actors including social media platforms, search engines, content hosting platforms and Internet Service Providers that you have identified?

Best practices and technological solutions

9. What are some best practices or examples you can share on creating:

(a) Educational curriculums within institutions that teach children and youth' online safety

(b) Awareness programs targeted at children, parents, and schools outside of teaching time

(c) National legislation and policy designed to identify and tackle risks to children and youth?

10. Are there any technological solutions (applications or other tools) that have been deployed by governments or other actors in your countries to improve cyber resilience among younger adults?

General

11. What information do you feel would be most useful to include in the toolkit on preventing online harms to children and younger adults?

12. Is there any other data, insight or best practice not covered by the questions above that you would like to share with us?

End of Toolkit