CHILD ONLINE SAFETY TOOLKIT

MAKING CHILD ONLINE SAFETY A REALITY

5RIGHTS FOUNDATION

End Violence Against Children

About 5Rights Foundation

Building the Digital World Young People Deserve

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world.

Our focus is on implementable change and our work is cited and used widely around the world. We work with governments, intergovernmental institutions, professional associations, academics, businesses, NGOs and children so that digital products and services can impact positively on the lived experiences of young people. A child or a young person is anyone under the age of 18, as defined by the UN Convention on the Rights of the Child.

This publication has been produced with financial support from the End Violence Fund, through its Safe Online initiative. The End Violence Fund provides financial support to programmes that deliver practical, innovative solutions to protect children from online exploitation and abuse. The opinions, findings, conclusions, and recommendations expressed herein are those of 5Rights Foundation and do not necessarily reflect those of the End Violence Fund.

5RIGHTS FOUNDATION

End Violence Against Children

Contents Page

● = Head here for key information

○○○ PREFACE ✕

“In this unprecedented moment, the power, promise and peril of digital technology cannot be underestimated. Coming together will allow the international community to ensure that technology is harnessed for good, seek the opportunity to manage its impact and ensure that it presents a level playing field for all.

Future generations will judge whether the present generation seized the opportunities presented by the age of digital interdependence. The time to act is now.”

António Guterres
United Nations Secretary-General
Secretary-General’s Roadmap for Digital Cooperation, June 2020

○○○ PREFACE ✕

“We cannot build a sustainable future unless we are able to ensure children can grow up safe and secure from violence and harm, including in digital environments. While in principle we all have a vision of what a safe and enabling digital world should look like for children, it becomes much more complex once we start translating those into actual policies, regulation, actions, products and services.

Our hope is that this Child Online Safety Toolkit is part of the solution to this problem – a practical guide for policy makers that simplifies key issues that we need to tackle if we are to make the internet safe for children.”

Dr. Howard Taylor
Executive Director
Global Partnership to End Violence Against Children

○○○ SYSTEM FOLDER ✕

8 ITEMS | 105 MB IN DISK | SECTION 1

NEXT SECTION >

Introduction

In an increasingly connected world, the need for a safe and enabling digital environment for children has never been greater. Policy makers across the globe are working to define the rules of engagement between children and the digital world. Nowhere is this highlighted more than in the publication of the UN Secretary-General's Digital Cooperation Roadmap.[1] This Toolkit is designed to support policy makers and practitioners, offering an accessible, practical approach to building a digital world that supports children, enabling them to flourish both online and beyond.

The Toolkit outlines the roadmap necessary to ensure the digital world is safe for and respectful of the rights of children. It separates its obligations into ten subject areas to support the implementation of the following key international agreements and frameworks: the Sustainable Development Goals (SDGs); the UNCRC General comment No. 25 (2021) on children's rights in the digital environment; the WeProtect Global Alliance Model National Response; and the International Telecommunication Union's Guidelines on Child Online Protection.

This Toolkit does not seek to replace any existing regional, national or international agreements and frameworks, but rather provides best practice examples from around the world, signposts detailed approaches across each policy area, and sets out the actions that individuals and teams charged with the task of protecting children online must take. As such, it is a tool for policy makers from across the world to embrace the obligations that they already have.

Guaranteeing online safety is not just about responding to risks and harms: it means actively designing a digital environment that is safe for every child. With one in three people online under the age of 18, the centrality of digital technology in children's lives means that it must be formed with their privacy, safety and rights by design and by default. This preventative and holistic approach is reflected within the Toolkit, providing a roadmap for governments, nation-states and organisations to build, review or improve their policies and practices with respect to children's rights. This will allow all in the chain of responsibility to play their part in working towards a global approach to child online safety which will evolve over time. The Toolkit is designed to be used by policy makers around the world, including those in newly connecting countries, and to be accessible and transferable to different contexts and settings.

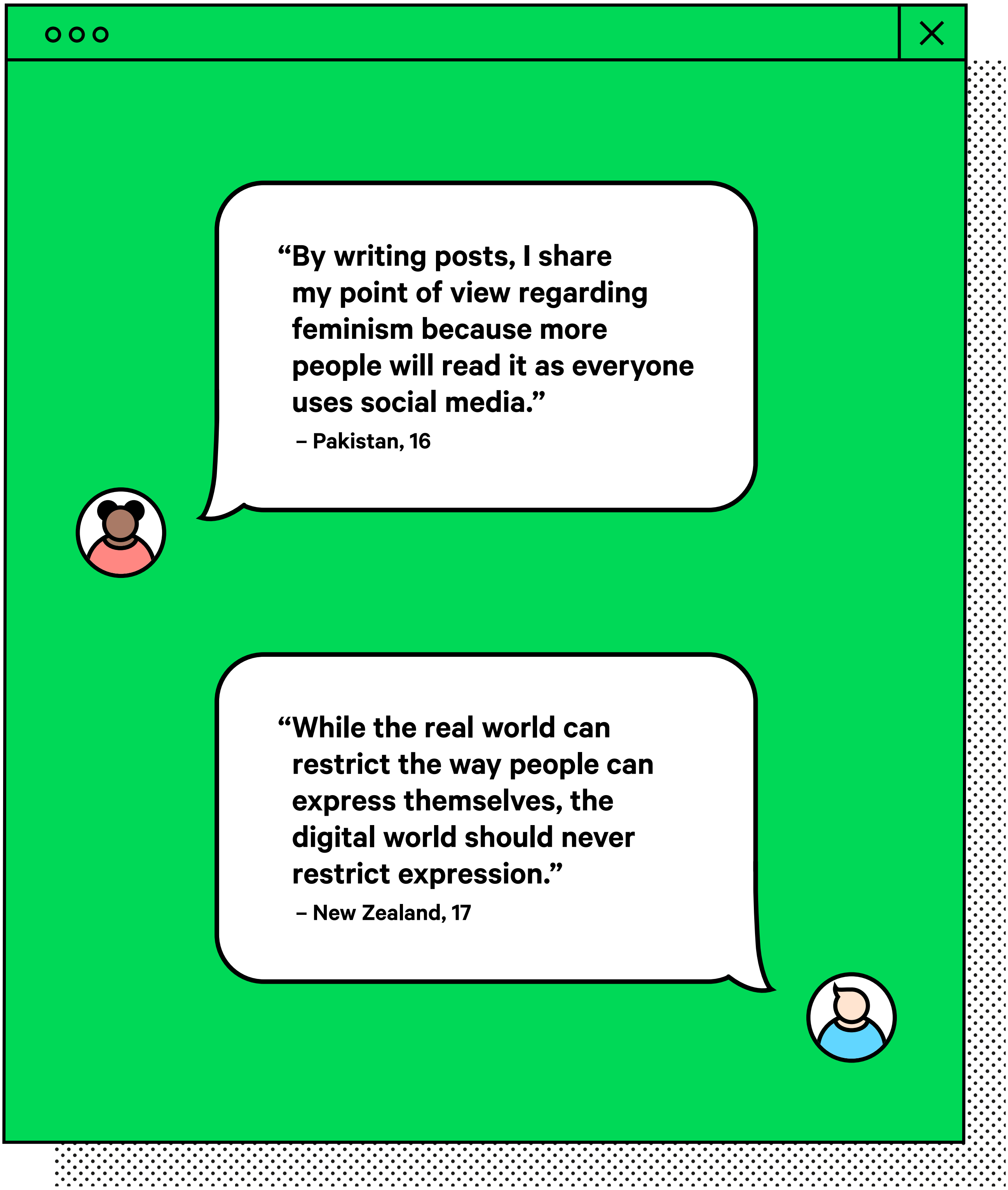
On behalf of 5Rights and our community, I want to thank Secretary-General *António Guterres* for his visionary leadership in providing a roadmap for a connected world and for recognising that if the connected world is not safe and rights-respecting for children, it will not fulfil its promise of a better world for all. I also wish to recognise that the initial work upon which this Toolkit is based was undertaken on behalf of the Government of Rwanda, and we are grateful for their support in allowing us to use it here. We are also grateful to Professor Julia Davidson OBE and Dr Susie Alegre for their contributions to this document. We also wish to acknowledge the generous support of the End Violence Fund, which enabled us to develop the Child Online Protection Policy for the Government of Rwanda, and which subsequently saw the potential to turn it into something that all countries could benefit from.

The Toolkit owes its wisdom and structure to the work of many others. These include, among others, the UN Committee on the Rights of the Child, WeProtect Global Alliance, End Violence Fund, University of East London, University of Rwanda, 5Rights Foundation and the many states, global intergovernmental organisations and academic, child protection and enforcement communities upon whose work it is built. We recognise all of them and thank them for their work, commitment and contributions. Above all, it owes its approach to the hundreds of children and young people who have told us they wish to engage with the digital world, creatively, safely and fearlessly: this Toolkit is theirs.

Baroness Beeban Kidron OBE
Founder and Chair, 5Rights Foundation

[1] United Nations Secretary-General's Roadmap for Digital Cooperation, United Nations, 2020.

NEXT SECTION >



“By writing posts, I share my point of view regarding feminism because more people will read it as everyone uses social media.”

– Pakistan, 16

“While the real world can restrict the way people can express themselves, the digital world should never restrict expression.”

– New Zealand, 17

SYSTEM FOLDER

8 ITEMS | 105 MB IN DISK | SECTION 2

< PREVIOUS SECTION NEXT SECTION >

How to use it

The Child Online Safety Toolkit provides practical tools to help policy makers from across the world fulfil their international obligations on children's rights and child online safety.

For some this document will be a starting point, for others it will provide an opportunity to check their current policy and implementation against international best practice. It is designed to be 'country-neutral', so that policy makers, working with an analysis of their own national context, can use it to assess and inform their own journey to embedding children's rights in the digital environment.

The Toolkit includes:

□ A comprehensive and robust 'model' policy on children's online safety as one approach that policymakers can implement or build on to ensure effective coordination across jurisdictions

□ Ten policy action areas for policy makers to use in developing their own child online safety policy

□ Checklists and other auditing tools that policy makers can use to assess and improve their country's current and planned actions for child online safety

□ Summaries and guidelines to global foundational documents

□ A glossary of key terms used in online safety and child online safety policy

□ Signposts to best practice examples and information from various countries

□ Diagrams and other explanatory materials to help communicate policy ideas to other audiences, including civil servants and civil society.

It responds to the call for action of the UN Secretary-General in his Roadmap for Digital Cooperation (2020) by bringing together foundational resources: the UNCRC's General comment No. 25 (2021); the International Telecommunication Union's Guidelines on Child Online Protection; and WeProtect Global Alliance's Model National Response, to provide a practical resource for policy makers to ensure child online safety.

The Toolkit and its resources are available online at childonlinesafetytoolkit.org and by contacting info@5rightsfoundation.com.

< PREVIOUS SECTION NEXT SECTION >

Language matters. The words we use affect the way we think about children's rights and children's online safety. The words we use affect how we prioritise issues, how we respond, and also, importantly, our ability to effectively collaborate and enforce or honour children's rights across borders. While national contexts may necessarily be different, it is essential that laws and regulations to the greatest extent possible use concepts, language and definitions that are aligned and allow for cooperation between law enforcement agencies, as well as cross-border cooperation and understanding more broadly.[2] The Toolkit includes internationally recognised glossaries from the UN Committee on the Rights of the Child and the Luxembourg Guidelines, which help provide a template for the language used.[3]

The Toolkit complements and highlights already well-developed models to support specific aspects of child online safety.

Foundational resources include:

- General comment No. 25 (2021) on children's rights in relation to the digital environment is a crucial tool for understanding children's rights in the context of child online safety. In it, the UN Committee on the Rights of the Child explains how states should implement the Convention on the Rights of the Child in relation to the digital environment and provides guidance on relevant legislative, policy and other measures to ensure full compliance with their obligations under the Convention and the Optional Protocols.[4]

- The WeProtect Global Alliance's *Model National Response* (MNR) is of particular importance in relation to child sexual exploitation and abuse (CSEA). The MNR is a key part of any national toolkit for child online safety.[5] The MNR is focused on helping countries to build their response to online child sexual exploitation and abuse, but it indicates that this cannot be addressed in isolation and states that a wider set of capabilities to prevent and tackle child sexual exploitation and abuse are required to be in place to ensure a complete national response. This Toolkit provides resources that support implementation of the MNR. The Child Online Safety Toolkit can help signatories of WeProtect Global Alliance's MNR to ensure that they have the institutional capacity to deliver on its goals and ensure obligations under the General comment are met.

- The International Telecommunication Union's (ITU) *Guidelines on Child Online Safety* 2020 are a comprehensive set of recommendations and tools for all relevant stakeholders on how to contribute to the development of a safe and empowering online environment for children and young people. They are tailored to four key audiences: children, parents/carers and educators, industry and policy makers. For each of these audiences, the guidelines are meant to act as a blueprint which can be adapted and used in a way that is consistent with national or local customs and laws, and address issues that might affect all children and young people under the age of 18.[6]

[2] "The Committee recommends that States parties, in establishing their legal frameworks, take into account technological advancements to ensure that their applicability is not eroded by future developments and to avoid loopholes associated with emerging concerns, including new forms of online sale and sexual exploitation. In light of the evolving nature of the issue, States parties should regularly assess and, when necessary, revise legislation and policies to guarantee that their legal and policy frameworks are adapted to rapidly changing realities." Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, United Nations Committee on the Rights of the Child, 2019.

[3] Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International, 2016.

[4] Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, WeProtect Global Alliance, 2015.

[5] General comment No. 25 on children's rights in relation to the digital environment, UNRC 2021.

[6] Guidelines on Child Online Protection, International Telecommunication Union, 2020.

< PREVIOUS SECTION NEXT SECTION >

Other important resources and frameworks relevant for policy makers looking at child online safety include:

□ **The UN *Sustainable Development Goals*.** The 17 Sustainable Development Goals (SDGs) are at the heart of the 2030 Agenda for Sustainable Development,[7] adopted by all United Nations Member States in 2015.

□ **The UN's *Guiding Principles on Business and Human Rights.***[8] These principles set out the obligations on States parties and on businesses to protect and respect human rights, including children's rights.

□ **The World Health Organization's *INSPIRE: Seven Strategies for Ending Violence Against Children.***[9] INSPIRE is an evidence-based technical package to support countries in their efforts to prevent and respond to violence against children.

□ **UNICEF's *Draft Policy Guidance on AI for Children.***[10] The Guidance is designed to promote children's rights in government and private sector AI policies and practices, and to raise awareness of how AI systems can uphold or undermine these rights.

There are many others on the regional, national and international level that may be relevant to specific country contexts or provide globally relevant models, many of which are cited in relevant sections of this Toolkit.

The prevalence of child sexual exploitation and abuse is also a major concern. In 2020, 65 million pieces of child sexual abuse material were reported to the National Center for Missing and Exploited Children of the United States, while many more went undetected.[11] The international community has long stood united in its shared resolve to protect children. Building on that resolve, cooperation between national law enforcement agencies and major technology companies has increased, but more can be done.

Companies must embrace more robust scanning practices and accelerate detection methods focused on prevention. This approach must also be supported by important legislative steps. In that regard, multi-stakeholder partnerships, such as the WeProtect Global Alliance and the Global Partnership to End Violence Against Children, are of great benefit.

Source: United Nations Secretary-General's Roadmap for Digital Cooperation, June 2020[12]

[7] Transforming our world: the 2030 Agenda for Sustainable Development, United Nations, 2021.

[8] Guiding Principles on Business and Human Rights, Office of the United Nations High Commissioner for Human Rights, 2011.l

[9] INSPIRE: Seven strategies for ending violence against children, World Health Organization, 2021.

[10] Policy guidance on AI for children, United Nations Children's Fund, 2020.

[11] CyberTipline Report, National Center for Missing and Exploited Children, 2020.Transforming our world: the 2030 Agenda for Sustainable Development, United Nations, 2021.

[12] United Nations Secretary General's Roadmap for Digital Cooperation, United Nations, June 2020.

< PREVIOUS SECTION NEXT SECTION >

How we made it

The digital world is constantly changing. Child online safety policy must be rooted in a child rights approach and must be sufficiently flexible to meet evolving risks and opportunities as they arise. The Child Online Safety Toolkit seeks to meet this need by providing a comprehensive set of actions for an adoptable policy, examples of best practice and resources that can be shared.

The Toolkit is the product of consultation from across the globe, taking account of insights from every continent, and locations ranging from small-island developing states to large industrial nations and everything in between.[13] We have consulted international experts from a range of backgrounds, including industry, policy makers and academics. The drafting was undertaken by 5Rights, which is headquartered in the UK, and was supported by colleagues in Europe, North America and Australia and by partners[14] who facilitated focus groups in Latin America, Africa and Asia, to ensure the Toolkit is both practical and relevant for a variety of local contexts. The text is rooted in global standards, in particular the UN Convention on the Rights of the Child, but the Toolkit can also be adapted to reflect the cultures and values found in national constitutions around the world.

It is a holistic, practical and accessible Toolkit for policy makers to pave the way for a world where all children feel safe and fulfilled: a world that has full respect for their rights both online and offline.

During consultations, children expressed the view that the digital environment should support, promote and protect their safe and equitable engagement:

“We would like the government, technology companies and teachers to help us to manage untrustworthy information online.”
- Ghana, unknown age

“I would like to obtain clarity about what really happens with my data ... Why collect it? How is it being collected?”
- Germany, 16

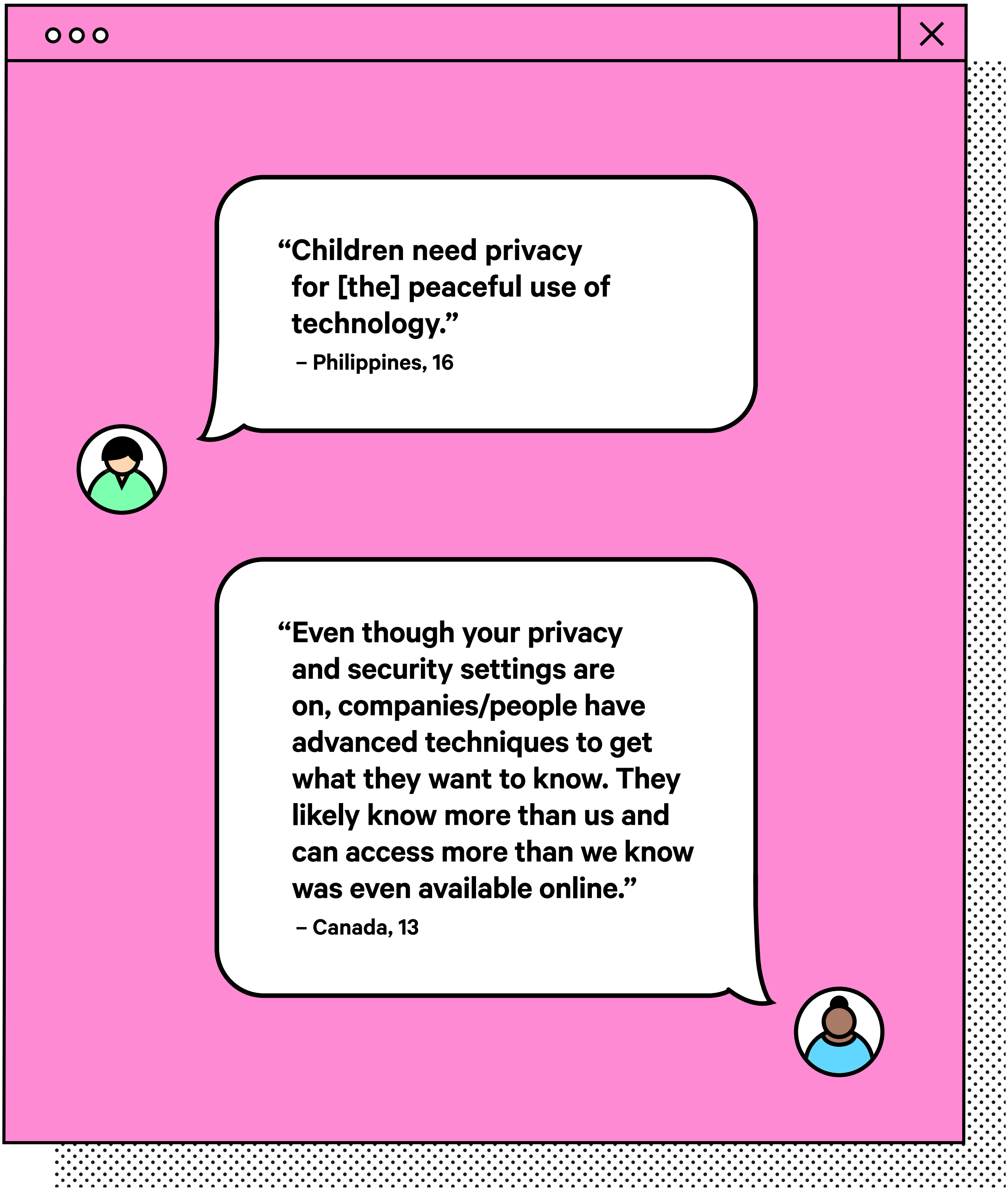
“I am ... worried about my data being shared.”
- Canada, 15

[13] Including focus group consultations in Brazil, Cambodia, Colombia, Ghana, Sri Lanka and Zimbabwe, to ensure that it has global relevance.

[14] Local partners included RedPapaz in Colombia, Alana Foundation in Brazil, African Digital Rights Hub in Ghana, UNICEF Zimbabwe, UNICEF Cambodia, and Save the Children International in Sri Lanka.

< PREVIOUS SECTION

NEXT SECTION >

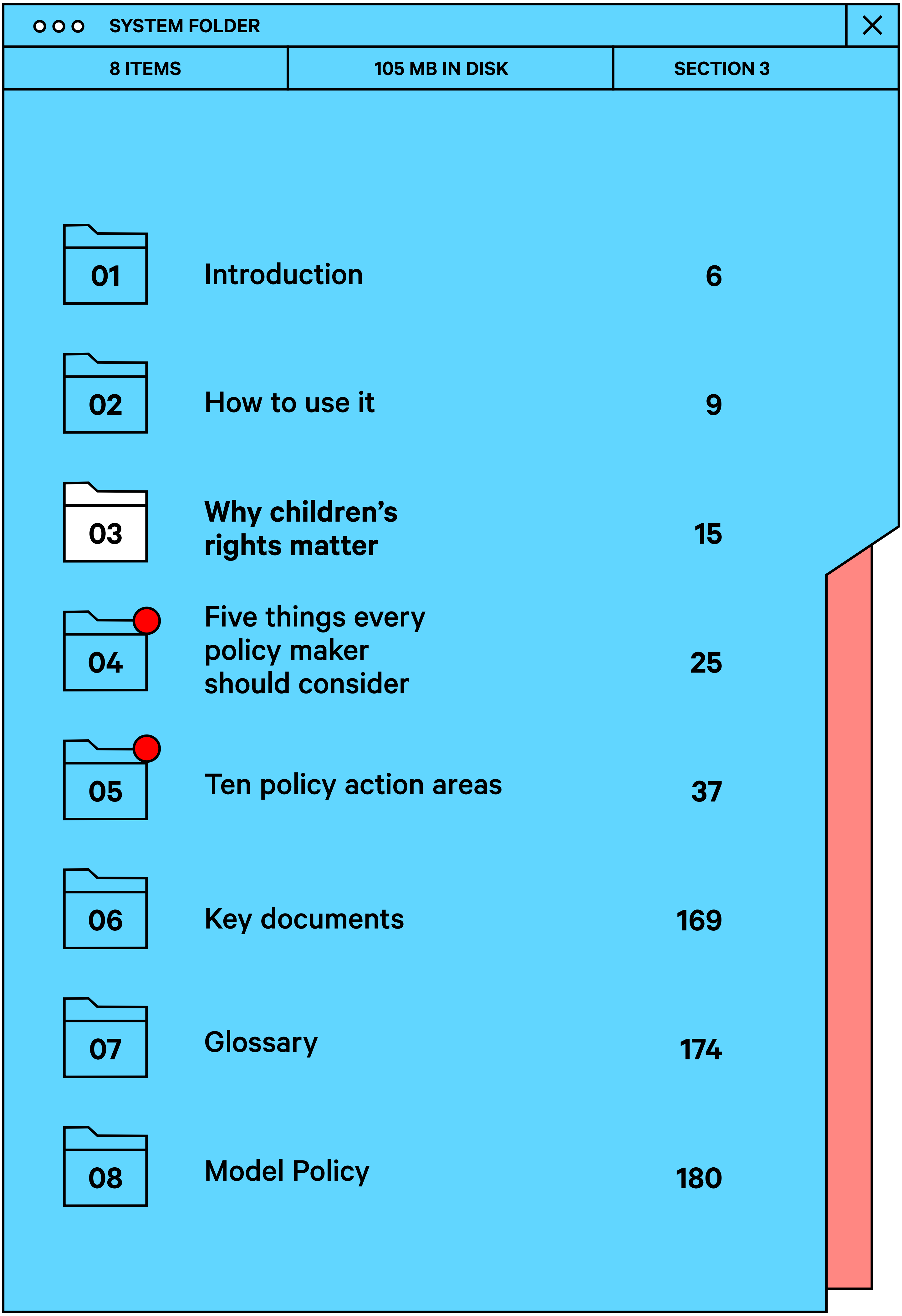


"Children need privacy for [the] peaceful use of technology."

– Philippines, 16

"Even though your privacy and security settings are on, companies/people have advanced techniques to get what they want to know. They likely know more than us and can access more than we know was even available online."

– Canada, 13



SYSTEM FOLDER
8 ITEMS
105 MB IN DISK
SECTION 3

< PREVIOUS SECTION NEXT SECTION >

Why children's rights matter

Children's rights provide a thread which runs through all policy that affects children's lives, both online and offline. The aim of a child online safety policy is, fundamentally, to make children's rights to protection and participation real and effective as they engage with the digital world.

Children and their families have human rights under the International Bill of Rights, including the Universal Declaration on Human Rights 1948, the International Covenant on Civil and Political Rights 1966 and the International Covenant on Economic, Social and Cultural Rights 1966, as well as regional and national human rights structures.

Specific to children, the *United Nations Convention on the Rights of the Child 1989* ('the Convention' or CRC)[15] along with its *Optional Protocols on the Sale of Children*[16] and *Children in Armed Conflict*[17] provide a practical framework for understanding how human rights apply to children. The Convention is the most widely ratified human rights treaty in history and its Optional Protocol on a Communications Procedure helps to make it enforceable so that children's rights are real and effective.

All rights contained in the CRC are relevant to child online safety, and consulting children is crucial to understanding what those rights mean in practice. For example, children's rights to play, participation and to family life in the online space should be considered. All those involved in carrying out consultations should be properly trained on children's rights and what children's voices and inclusion means in practice.

The United Nations Committee on the Rights of the Child[18] provides guidance – in General comment No. 25 (2021) – on legislative, policy and other appropriate measures to ensure full compliance with the obligations under the Convention and its Optional Protocols in light of the opportunities, risks and challenges for children's rights in the digital environment. The General comment No. 25 (2021) will be a key tool to consider when developing a child online safety policy.

> **The rights of every child must be respected, protected and fulfilled in the digital environment. Innovations in digital technologies affect children's lives and their rights in ways that are wide-ranging and interdependent, even where children do not themselves access the Internet. Meaningful access to digital technologies can support children to realise the full range of their civil, political, cultural, economic and social rights. However, if digital inclusion is not achieved, existing inequalities are likely to increase, and new ones may arise.**
>
> Source: General comment No. 25 (2021), para 4[19]

[15] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989.

[16] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989.

[17] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989.

[18] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC United Nations Committee on the Rights of the Child, 2021.

[19] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC United Nations Committee on the Rights of the Child, 2021.

< PREVIOUS SECTION NEXT SECTION >

The CRC gives four guiding principles for the protection of children's rights, and General comment No. 25 (2021) describes how these apply in the digital world:

1. The right to non-discrimination (article 2):

Article 2 of the Convention on the Rights of the Child[20] outlines that every child has the right to enjoy their rights equally, "without discrimination of any kind, irrespective of the child's or his or her parent's or legal guardian's race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status". Paragraphs 10 and 11 in the General comment No. 25 (2021) outline how this applies in the digital world.

> **Children may be discriminated against by their being excluded from using digital technologies and services or by receiving hateful communications or unfair treatment through use of those technologies. Other forms of discrimination can arise when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child.**
>
> **The Committee calls upon States parties to take proactive measures to prevent discrimination on the basis of sex, disability, socioeconomic background, ethnic or national origin, language or any other grounds, and discrimination against minority and indigenous children, asylum-seeking, refugee and migrant children, lesbian, gay, bisexual, transgender and intersex children, children who are victims and survivors of trafficking or sexual exploitation, children in alternative care, children deprived of liberty and children in other vulnerable situations. Specific measures will be required to close the gender-related digital divide for girls and to ensure that particular attention is given to access, digital literacy, privacy and online safety.**
>
> Source: General comment No. 25 (2021), paras 10-11[21]

[20] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, United Nations, 1989.

[21] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

2. The best interests of the child (article 3, paragraph 1):

Article 3 of the Convention on the Rights of the Child[22] states that "in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration". Paragraphs 12 and 13 in General comment No. 25 (2021) outline how this applies in the digital world.

> **The best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context. The digital environment was not originally designed for children, yet it plays a significant role in children's lives. States parties should ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration.**
>
> **States parties should involve the national and local bodies that oversee the fulfilment of the rights of children in such actions. In considering the best interests of the child, they should have regard for all children's rights, including their rights to seek, receive and impart information, to be protected from harm and to have their views given due weight, and ensure transparency in the assessment of the best interests of the child and the criteria that have been applied.**
>
> Source: General comment No. 25 (2021), paras 12-13[23]

3. Right to life, survival, and development (article 6):

Article 6 of the Convention on the Rights of the Child[24] requires that States parties "recognise that every child has the inherent right to life" and that they must "ensure to the maximum extent possible the survival and development of the child". Paragraph 15 in General comment No. 25 (2021) outlines how this applies in the digital world.

> **The use of digital devices should not be harmful, nor should it be a substitute for in-person interactions among children or between children and parents or caregivers. States parties should pay specific attention to the effects of technology in the earliest years of life, when brain plasticity is maximal and the social environment, in particular relationships with parents and caregivers, is crucial to shaping children's cognitive, emotional and social development. In the early years, precautions may be required, depending on the design, purpose and uses of technologies. Training and advice on the appropriate use of digital devices should be given to parents, caregivers, educators and other relevant actors, taking into account the research on the effects of digital technologies on children's development, especially during the critical neurological growth spurts of early childhood and adolescence.**
>
> Source: General comment No. 25 (2021), para 15[25]

[22] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, United Nations, 1989.

[23] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[24] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, United Nations, 1989.

[25] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

4. The right to be heard (article 12):

Article 12 of the Convention on the Rights of the Child[26] requires States parties to ensure that where children are "capable of forming (their) own views" they must enjoy "the right to express those views freely in all matters affecting (them)" and that these views must be given "due weight in accordance with the age and maturity of the child". Paragraph 17 in General comment No. 25 (2021) outlines how this applies in the digital world, and more information about how to implement this right can be found in the Resources 1 below.

> **When developing legislation, policies, programmes, services and training on children's rights in relation to the digital environment, States parties should involve all children, listen to their needs and give due weight to their views. They should ensure that digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services.**
>
> Source: General comment No. 25 (2021), para 17 [27]

These principles are indivisible and should all be borne in mind when developing a child online safety policy. They provide a useful lens through which to consider what the other five cross-cutting themes mean in practice and how the ten policy action areas outlined in the Toolkit should be delivered.

Children's rights are not only found in international law. Most national constitutions or legal frameworks include general human rights provisions that protect children. These national human rights laws should also be used in developing child online safety policy that puts the protection and promotion of children's rights at its heart.

The UN Committee on the Rights of the Child calls on States to ensure that national policies relating to children's rights should specifically address the digital environment and that children's online protection is integrated within national child protection policies. This Toolkit is designed to help them to do that.

[26] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, United Nations, 1989.

[27] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

> **States parties should ensure that national policies relating to children's rights specifically address the digital environment, and they should implement regulation, industry codes, design standards and action plans accordingly, all of which should be regularly evaluated and updated. Such national policies should be aimed at providing children with the opportunity to benefit from engaging with the digital environment and ensuring their safe access to it.**
>
> **Children's online protection should be integrated within national child protection policies. States parties should implement measures that protect children from risks, including cyberaggression and digital technology-facilitated and online child sexual exploitation and abuse, ensure the investigation of such crimes and provide remedy and support for children who are victims. They should also address the needs of children in disadvantaged or vulnerable situations, including by providing child-friendly information that is, when necessary, translated into relevant minority languages.**
>
> **States parties should ensure the operation of effective child protection mechanisms online and safeguarding policies, while also respecting children's other rights, in all settings where children access the digital environment, which includes the home, educational settings, cybercafés, youth centres, libraries and health and alternative care settings.**
>
> Source: General comment No. 25 (2021), paras 24-26 [28]

Resources for children's rights:

1. Implementing the right to be heard in developing your child online safety policy:

The right to be heard must be at the heart of practical policy making on child online safety. Children and young people have strong opinions on the digital environment[29], and they have a right to be heard in matters that affect them.[30] For child online safety policy to address children's needs, policy makers must hear children's voices and include their perspectives in policy making. Children's perspectives on risk and harms, benefits and opportunities in the online environment may be different from those of the adults around them. Effective consultation with child participation[31] throughout the development, implementation, monitoring and evaluation of child online safety policies is therefore crucial in order to ensure their needs are properly met and to ensure that the policy is truly child-friendly.[32]

[28] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[29] In our own words – children's rights in the digital world, 5Rights Foundation, 2021.

[30] The right to be heard is contained in Article 13 of the Convention.

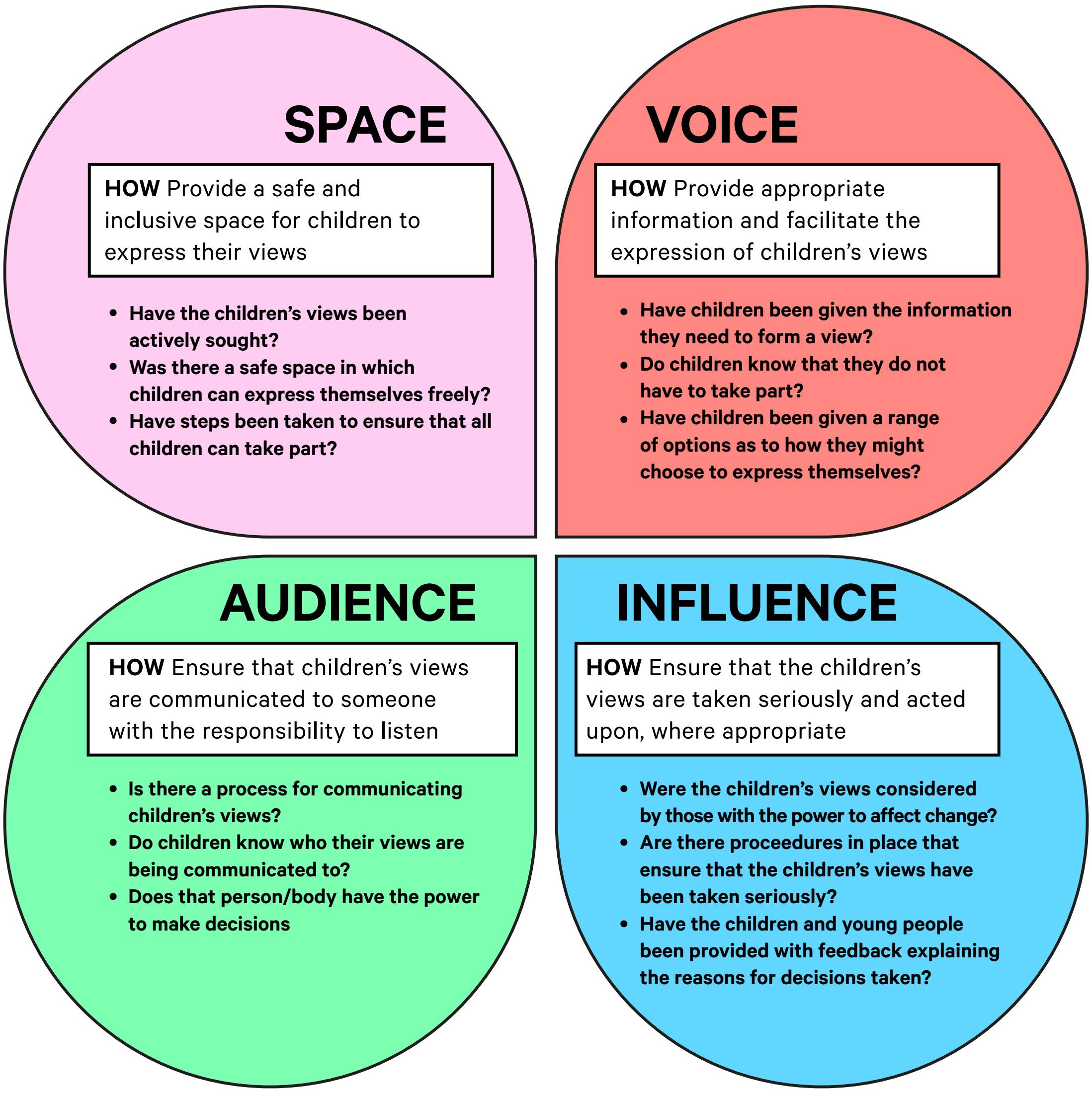
[31] This should take into account the four elements of the Lundy Model: space, voice, audience, influence. See: The Lundy model of child participation.

[32] The Digital Futures Commission.

< PREVIOUS SECTION

NEXT SECTION >

The Lundy model presents one method of understanding 'how to' enable children's participation, through four areas of focus:



SPACE

HOW Provide a safe and inclusive space for children to express their views

- **Have the children's views been actively sought?**
- **Was there a safe space in which children can express themselves freely?**
- **Have steps been taken to ensure that all children can take part?**

VOICE

HOW Provide appropriate information and facilitate the expression of children's views

- **Have children been given the information they need to form a view?**
- **Do children know that they do not have to take part?**
- **Have children been given a range of options as to how they might choose to express themselves?**

AUDIENCE

HOW Ensure that children's views are communicated to someone with the responsibility to listen

- **Is there a process for communicating children's views?**
- **Do children know who their views are being communicated to?**
- **Does that person/body have the power to make decisions**

INFLUENCE

HOW Ensure that the children's views are taken seriously and acted upon, where appropriate

- **Were the children's views considered by those with the power to affect change?**
- **Are there proceedures in place that ensure that the children's views have been taken seriously?**
- **Have the children and young people been provided with feedback explaining the reasons for decisions taken?**

Source: The Lundy model of child participation[33]

The involvement of children's voices and experiences when drafting a child online safety policy is reiterated by the International Telecommunication Union's Guidelines on Child Online Protection. Ensuring the voices of children are incorporated into any consideration of child online safety allows for a more robust, diverse and inclusive policy.

> **Children and young people want to be involved in the conversation, and they have valuable expertise as 'digital natives' that can be shared. Policy-makers and practitioners must engage with children and young people in an on-going debate about the online environment to support their rights.**
>
> Source: ITU Guidelines for policy-makers on Child Online Protection 2020[34]

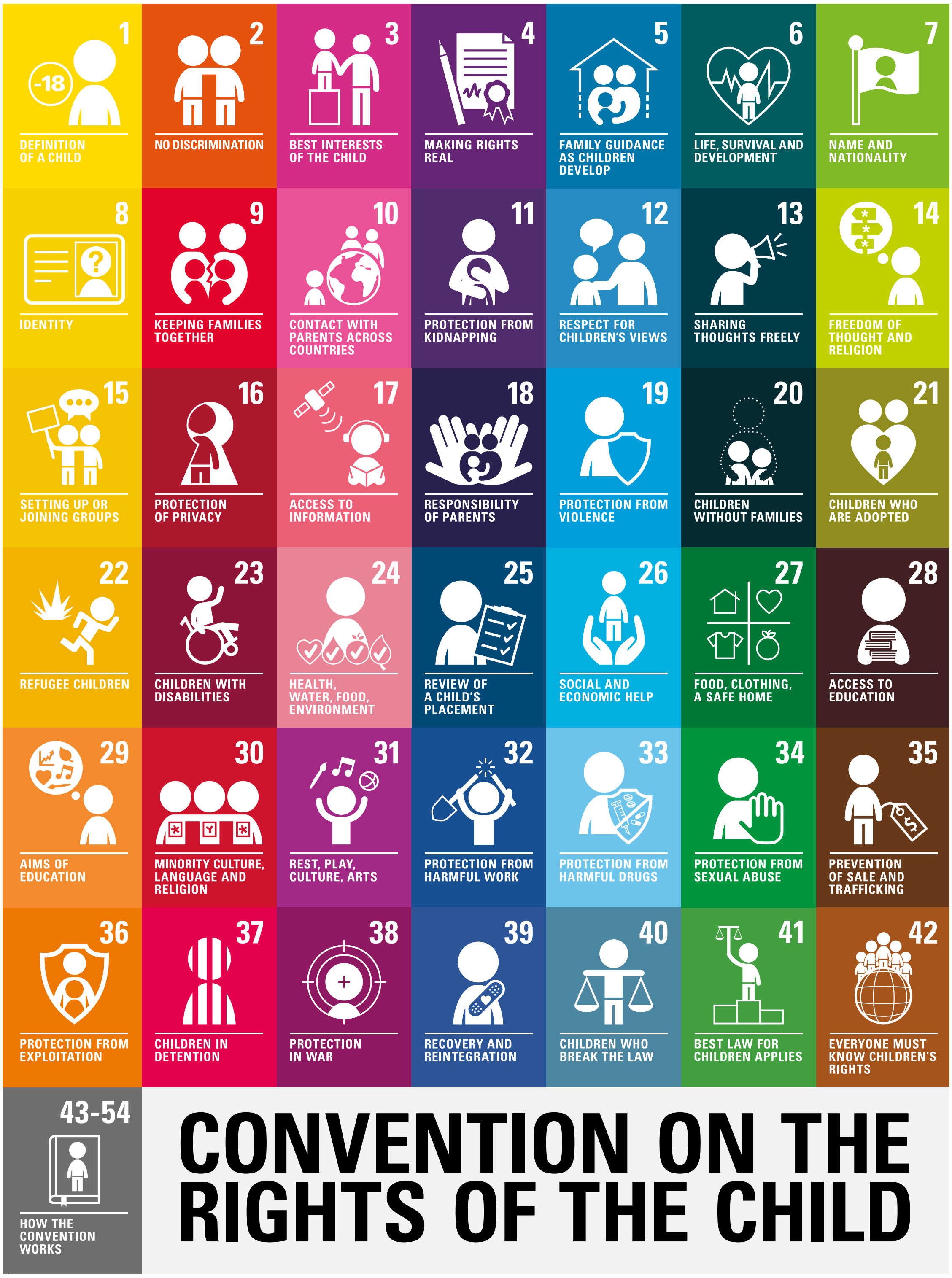
[33] The Lundy model of child participation, European Commission, 2007.

[34] Guidelines for policy-makers on Child Online Protection, International Telecommunication Union, 2020.

< PREVIOUS SECTION

NEXT SECTION >

2. Helping people understand the Convention on the Rights of the Child:


1 -18 DEFINITION OF A CHILD
2 NO DISCRIMINATION
3 BEST INTERESTS OF THE CHILD
4 MAKING RIGHTS REAL
5 FAMILY GUIDANCE AS CHILDREN DEVELOP
6 LIFE, SURVIVAL AND DEVELOPMENT
7 NAME AND NATIONALITY
8 IDENTITY
9 KEEPING FAMILIES TOGETHER
10 CONTACT WITH PARENTS ACROSS COUNTRIES
11 PROTECTION FROM KIDNAPPING
12 RESPECT FOR CHILDREN'S VIEWS
13 SHARING THOUGHTS FREELY
14 FREEDOM OF THOUGHT AND RELIGION
15 SETTING UP OR JOINING GROUPS
16 PROTECTION OF PRIVACY
17 ACCESS TO INFORMATION
18 RESPONSIBILITY OF PARENTS
19 PROTECTION FROM VIOLENCE
20 CHILDREN WITHOUT FAMILIES
21 CHILDREN WHO ARE ADOPTED
22 REFUGEE CHILDREN
23 CHILDREN WITH DISABILITIES
24 HEALTH, WATER, FOOD, ENVIRONMENT
25 REVIEW OF A CHILD'S PLACEMENT
26 SOCIAL AND ECONOMIC HELP
27 FOOD, CLOTHING, A SAFE HOME
28 ACCESS TO EDUCATION
29 AIMS OF EDUCATION
30 MINORITY CULTURE, LANGUAGE AND RELIGION
31 REST, PLAY, CULTURE, ARTS
32 PROTECTION FROM HARMFUL WORK
33 PROTECTION FROM HARMFUL DRUGS
34 PROTECTION FROM SEXUAL ABUSE
35 PREVENTION OF SALE AND TRAFFICKING
36 PROTECTION FROM EXPLOITATION
37 CHILDREN IN DETENTION
38 PROTECTION IN WAR
39 RECOVERY AND REINTEGRATION
40 CHILDREN WHO BREAK THE LAW
41 BEST LAW FOR CHILDREN APPLIES
42 EVERYONE MUST KNOW CHILDREN'S RIGHTS
43-54 HOW THE CONVENTION WORKS
CONVENTION ON THE RIGHTS OF THE CHILD

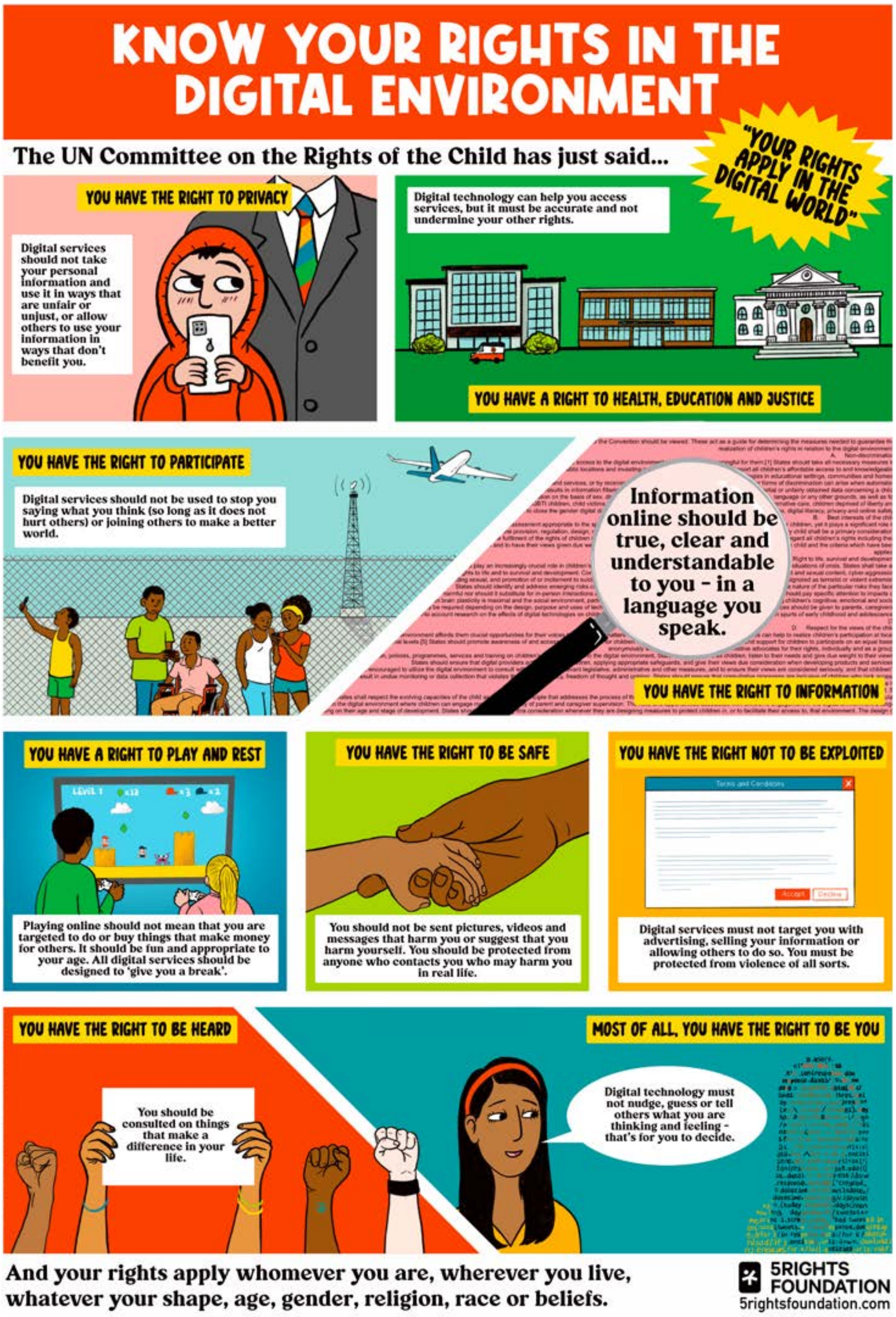
Source: The United Nations Convention on the Rights of the Child: The Children's Version[35]

[35] The United Nations Convention on the Rights of the Child: The Children's Version, Save the Children, 2019.

< PREVIOUS SECTION

NEXT SECTION >

3. Helping children understand General comment No. 25 (2021) on children's rights in relation to the digital environment:



KNOW YOUR RIGHTS IN THE DIGITAL ENVIRONMENT

The UN Committee on the Rights of the Child has just said...

"YOUR RIGHTS APPLY IN THE DIGITAL WORLD"

YOU HAVE THE RIGHT TO PRIVACY

Digital services should not take your personal information and use it in ways that are unfair or unjust, or allow others to use your information in ways that don't benefit you.

Digital technology can help you access services, but it must be accurate and not undermine your other rights.

YOU HAVE A RIGHT TO HEALTH, EDUCATION AND JUSTICE

YOU HAVE THE RIGHT TO PARTICIPATE

Digital services should not be used to stop you saying what you think (so long as it does not hurt others) or joining others to make a better world.

Information online should be true, clear and understandable to you - in a language you speak.

YOU HAVE THE RIGHT TO INFORMATION

YOU HAVE A RIGHT TO PLAY AND REST

Playing online should not mean that you are targeted to do or buy things that make money for others. It should be fun and appropriate to your age. All digital services should be designed to 'give you a break'.

YOU HAVE THE RIGHT TO BE SAFE

You should not be sent pictures, videos and messages that harm you or suggest that you harm yourself. You should be protected from anyone who contacts you who may harm you in real life.

YOU HAVE THE RIGHT NOT TO BE EXPLOITED

Digital services must not target you with advertising, selling your information or allowing others to do so. You must be protected from violence of all sorts.

YOU HAVE THE RIGHT TO BE HEARD

You should be consulted on things that make a difference in your life.

MOST OF ALL, YOU HAVE THE RIGHT TO BE YOU

Digital technology must not nudge, guess or tell others what you are thinking and feeling - that's for you to decide.

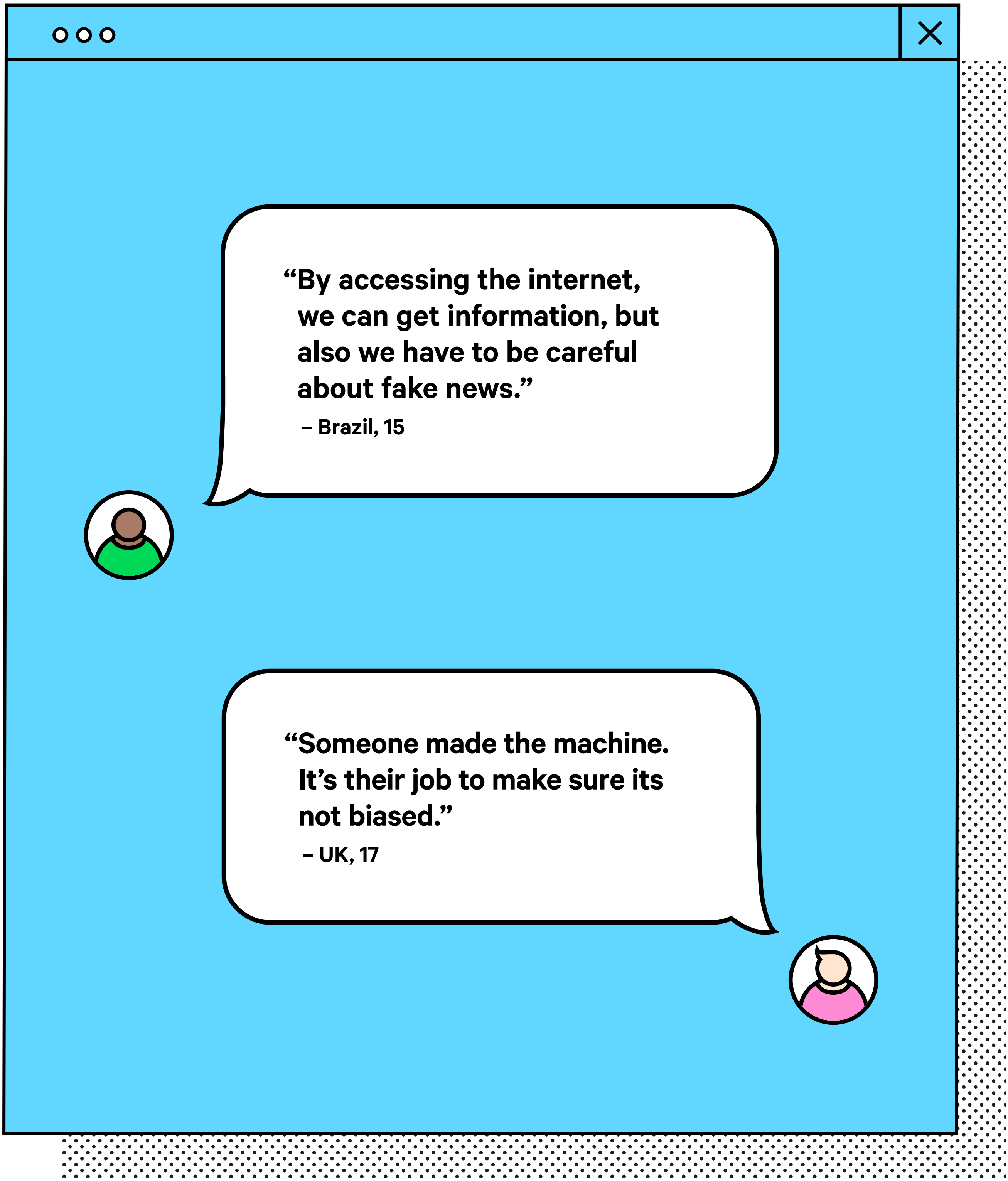
And your rights apply whomever you are, wherever you live, whatever your shape, age, gender, religion, race or beliefs.

5RIGHTS FOUNDATION
5rightsfoundation.com

Source: Know Your Rights! General comment No. 25 (2021) poster[36]

[36] Know Your Rights! General comment No. 25 (2021) posters, 5Rights Foundation, 2021.

< PREVIOUS SECTION NEXT SECTION >



"By accessing the internet, we can get information, but also we have to be careful about fake news."

– Brazil, 15

"Someone made the machine. It's their job to make sure its not biased."

– UK, 17

○○○ SYSTEM FOLDER ✕

8 ITEMS | 105 MB IN DISK | SECTION 4

< PREVIOUS SECTION NEXT SECTION >

The things every policy maker should consider

This section explores five cross-cutting themes that policy makers should think about when designing, developing and implementing child online safety policies.

○○○ FIVE THINGS

1. **Identifying risk and mitigating harm**
2. **Promoting access, accessibility and inclusion**
3. **Building a chain of responsibility and collaboration**
4. **Integrating child-centred design**
5. **Ensuring effectiveness**

Each of these issues should be considered when implementing the ten policy action areas on page no. 38.

1. Identifying risk and mitigating harm:

> **Opportunities provided by the digital environment play an increasingly crucial role in children's development and may be vital for children's life and survival, especially in situations of crisis. States parties should take all appropriate measures to protect children from risks to their right to life, survival and development. Risks relating to content, contact, conduct and contract encompass, among other things, violent and sexual content, cyberaggression and harassment, gambling, exploitation and abuse, including sexual exploitation and abuse, and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist. States parties should identify and address the emerging risks that children face in diverse contexts, including by listening to their views on the nature of the particular risks that they face.**
>
> Source: General comment No. 25 (2021), para 14[37]

Child online safety strategies must be developed primarily to maximise the benefits children can gain from digital technologies. This necessarily means that there is a prime responsibility to mitigate risks, minimise the likelihood of harm occurring, address harms where they have occurred, and consider how products and services may impact the end user, if that user is (or is likely to be) a child. Designing products and services that anticipate the safe participation of children is key.

[37] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

While acute harm is suffered by some children, millions of others experience online harm in one form or another. For example, there is a wide range of risks from commercial surveillance or exploitation, exposure to false information or scams, predators or bullying, while a lesser number suffer the acute harm of child sexual abuse. Many risks are cumulative. These impact different children in different ways and one form of harm may offer gateways to other forms of harm.[38]

The global nature of the online world means children face many of the same online risks regardless of their own geographical location. But different contexts can also raise specific concerns. In some cases, a child may be disadvantaged by a lack of access to the online environment; in other cases, there may be a link between harm that happens online with a child's offline experience. Specific risks and harms often overlap with each other. There are very few straight lines or neat divisions.

Factors such as gender, age, family circumstances, socioeconomic status, location, experiences and availability of digital technology, can alter the risks and the ways in which children experience harm. Some risks and harms affect whole communities and classes of children: for example, girls attract higher levels of abuse but for boys the abuse tends to be harsher.[39] Cultural norms surrounding masculinity also worsen the problem of under-detection and under-reporting of male child sexual abuse.[40] Risks and harms may also be amplified by platforms which are designed in a manner that encourages the sharing of shocking and sensational content – or they might profile or promote certain types of user behaviour because this drives profitable engagement.

Policymakers must consider all risks to children and take steps to mitigate them. A key tool to identify risk is the 4Cs framework.

The CO:RE 4Cs classification recognises that online risks arise when a child:

□ Engages with and/or is exposed to potentially harmful **content**

□ Experiences and/or is targeted by potentially harmful **contact**

□ Witnesses, participates in and/or is a victim of potentially harmful **conduct**

□ Is party to and/or exploited by a potentially harmful **contract**.

CO:RE	CONTENT Child as recipient	CONTACT Child as participant	CONDUCT Child as actor	CONTRACT Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualisation of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalisation and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

Source: CO:RE Content, Contact, Conduct, Contract – Updating the 4Cs of online risk, 2021 [41]

[38] Building the digital world that young people deserve, 5Rights Foundation, 2020.

[39] Safe Online Investment Portfolio Results 2020, Global Partnership to End Violence Against Children, 2020. p.2.

[40] Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse, Global Partnership to End Violence Against Children, 2021. p.68.

[41] Content, Contact, Conduct, Contract - Updating the 4Cs of Online Risk, CO:RE 2021.

< PREVIOUS SECTION NEXT SECTION >

> **With the expansion of affordable broadband to the developing world, there is an urgent need to put in place measures to minimise the risks and threats to these children, while also allowing them to capitalise on all the benefits of the digital world.**
>
> Source: ITU Guidelines for policy-makers on Child Online Protection 2020[42]

> **States parties should take into account the changing position of children and their agency in the modern world, children's competence and understanding, which develop unevenly across areas of skill and activity, and the diverse nature of the risks involved. Those considerations must be balanced with the importance of exercising their rights in supported environments and the range of individual experiences and circumstances. States parties should ensure that digital service providers offer services that are appropriate for children's evolving capacities.**
>
> Source: General comment No. 25 (2021), para 20[43]

2. Promoting access, accessibility and inclusion:

> **The rights of every child must be respected, protected and fulfilled in the digital environment. Innovations in digital technologies affect children's lives and their rights in ways that are wide-ranging and interdependent, even where children do not themselves access the internet. Meaningful access to digital technologies can support children to realise the full range of their civil, political, cultural, economic and social rights. However, if digital inclusion is not achieved, existing inequalities are likely to increase, and new ones may arise.**
>
> Source: General comment No. 25 (2021), para 4[44]

Today, access to the online world is crucial for children to realise their rights and achieve their full potential. A child online safety policy must be inclusive, both in aspiration and in practice.[45] This means that it must be adequately resourced and should build on existing best practice and frameworks, particularly in situations where resources are limited. Whether implementing child online safety policy means adapting existing legislation (e.g. regarding child protection, consumer protection or telecoms regulation) to the child online safety context or creating new bodies of law, it must promote inclusion and equality for all children, no matter who or where they are.

> **States parties should promote technological innovations that meet the requirements of children with different types of disabilities and ensure that digital products and services are designed for universal accessibility so that they can be used by all children without exception and without the need for adaptation. Children with disabilities should be involved in the design and delivery of policies, products and services that affect the realization of their rights in the digital environment.**
>
> Source: General comment No. 25 (2021), para 91[46]

[42] Guidelines for policy-makers on Child Online Protection, International Telecommunication Union, 2020.

[43] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[44] General comment No. 25 (2021) on children''s rights in relation to the digital environment, UNCRC, 2021.

[45] For example: children with disabilities or children from marginalised minority groups, street children, displaced children and migrant children, among others. This issue is further discussed in the cross-cutting themes below. More information on the model and the checklist can be found in 'Voice' is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child, Laura Lundy, 2013.

[46] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

Children are not a homogeneous group. Child online safety policies must be accessible and inclusive to reach all children, whoever and wherever they are. A "digital divide" is very likely to arise where some children have easy access to the online space, while others are effectively excluded. Frameworks need to be age-appropriate and work for all children regardless of gender, race, religion, nationality, ethnicity, disability or any other characteristics. Language should be accessible and inclusive and, where needed, materials should be available in a range of different languages. Child online safety materials should be developed in consultation with children and parents/carers: at a minimum, they should be age-appropriate, gender-neutral and easily accessible to children of different ages and their parents/carers. Where literacy is limited, visual materials will often get messages across much more effectively. Using consistent terms across platforms helps to make child online safety more easily understandable and accessible for children and their families and carers.[47]

Policy-makers must ensure they are promoting access for children online and including them in their journey in making digital environments safe.

> **Adults and children are exposed to a range of risks and dangers online. Nonetheless, children are a much more vulnerable population. Some children are also more vulnerable than other groups of children, for instance children with disabilities or children on the move. Policy makers need to guarantee that all children can develop and be educated in a safe digital environment. The idea that children are vulnerable and should be protected from all forms of exploitation is outlined in the UN Convention on the Rights of the Child.**
>
> Source: ITU Guidelines for policy-makers on Child Online Protection 2020[48]

3. Building a chain of responsibility:

> **To encompass the cross-cutting consequences of the digital environment for children's rights, States parties should identify a government body that is mandated to coordinate policies, guidelines and programmes relating to children's rights among central government departments and the various levels of government. Such a national coordination mechanism should engage with schools and the information and communications technology sector and cooperate with businesses, civil society, academia and organizations to realise children's rights in relation to the digital environment at the cross-sectoral, national, regional and local levels. It should draw on technological and other relevant expertise within and beyond government, as needed, and be independently evaluated for its effectiveness in meeting its obligations.**
>
> Source: General comment No. 25 (2021), para 27[49]

The responsibility for child online safety involves many people, specialisms and organisations – including government, law enforcement, business, educators, psycho-social support, families, and children. Some links in the chain bear a greater weight of responsibility.[50] For example, a service that is likely to be accessed by or impact on children should consider if any of its features pose a risk to children. They should do this before engaging with any child users. This is often referred to as 'safety by design', or 'child-centred design'. Safety by default should be the norm.

[47] See introduction on the importance of language and definitions and glossary section.

[48] Guidelines for policy-makers on Child Online Protection, International Telecommunication Union, 2020.

[49] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[50] See for example the UN Guiding Principles on Business and Human Rights.

< PREVIOUS SECTION NEXT SECTION >

Stakeholder chain of responsibility

Taking responsibility for child online safety includes both preventing the harm before it happens and taking action when things go wrong. Complaint and reporting mechanisms need to be accessible and clearly signposted so that children, carers and professionals who need them can find and use them easily. Within online business systems, mechanisms should be put in place which allow for reports of complaints to be monitored and evaluated so that areas of concern can be swiftly identified and addressed.

Laws and regulations need to establish clear frameworks for prevention and responsibility and redress when things go wrong. This includes collecting data about reports and complaints, so that they are monitored and analysed to improve the system. Children and parents/carers should not be made responsible for preventing or addressing risks and harms that they have little understanding or control over. Consent cannot be used to absolve public or private organisations from their responsibilities regarding child online safety. Integrating child online safety into existing frameworks for product safety[51], child protection[52], children's rights[53] and consumer rights[54] may help to avoid gaps in responsibility and duplication of resources, roles and responsibilities. There should, and must, be no legal loopholes that undermine effective child online safety.

It is vital that child online safety is embedded and integrated into all related policy areas, from national broadband plans to education curricula, in a way that is transparent, accountable and enforceable. Creating silos can lead to regulatory conflict and fragmented policy making and implementation.

Policy makers must embrace the complexity of responsibility for child online safety and ensure that there are mechanisms of cooperation and support for everyone in the chain, so that they can play their part in protecting children. A clear understanding of roles and responsibilities and leading actors for specific areas is also critical.

> **Protecting children and young people is a shared responsibility and it is upon all relevant stakeholders to ensure a sustainable future for all. For that to happen, policy makers, the industry, parents, carers, educators and other stakeholders, must ensure that children and young people can fulfil their potential – online and offline.**
>
> Source: ITU Guidelines for policy-makers on Child Online Protection 2020[55]

> **Good governance brings together those with a responsibility to protect children from online sexual exploitation and is a multi-stakeholder, cross-sector national body or bodies. There is no one model that the multi-stakeholder body should adopt: it might be responsible for the overall governance and oversight of a country's capability and capacity to prevent and respond to online CSEA, or simply act as a body for coordinating work across government, industry and civil society.**
>
> Source: WeProtect Global Alliance Model National Response 2016[56]

[51] Standards and risks for specific products, European Commission, 2014.

[52] Child Protection Hub, European Commission, 2021.

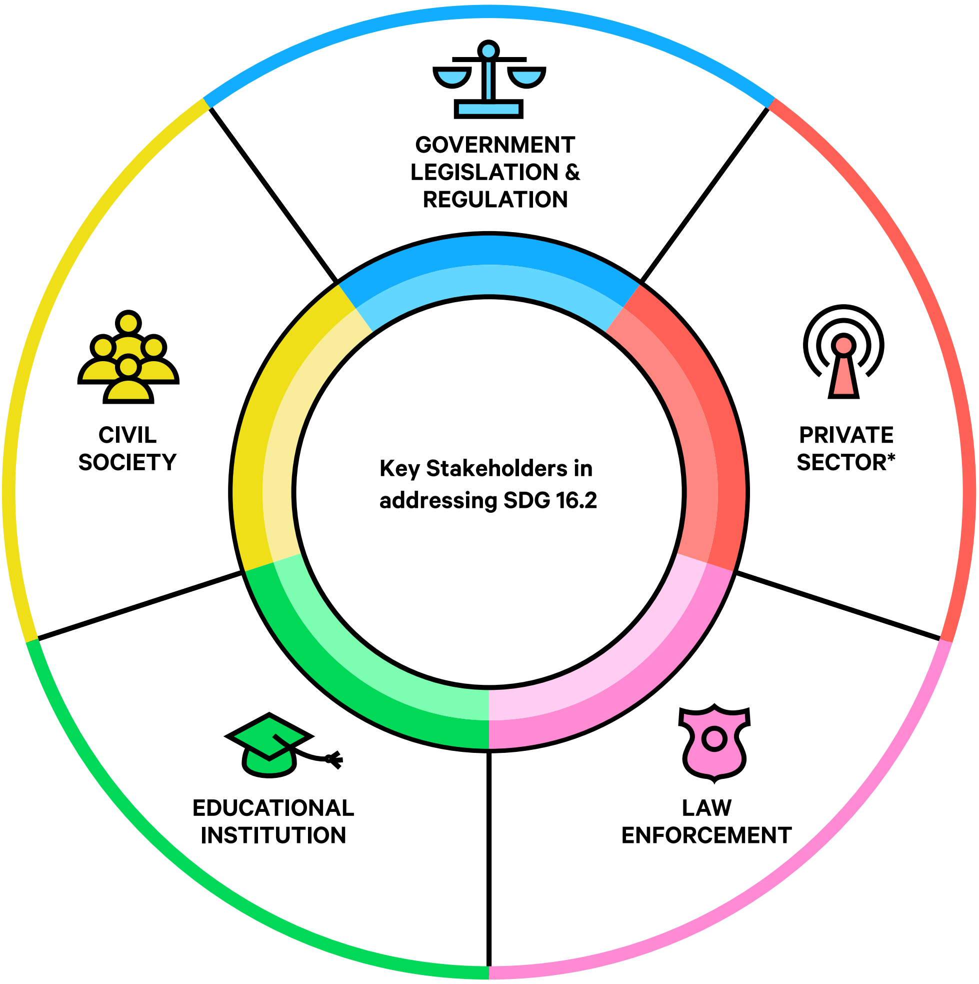
[53] Strategy for the Rights of the Child, Council of Europe, 2021.

[54] Consumer rights directive, European Commission, 2014.

[55] Guidelines for policy-makers on Child Online Protection, International Telecommunication Union, 2020.

< PREVIOUS SECTION NEXT SECTION >

These responsibilities are also reflected in other commitments, including the Sustainable Development Goals codified as Goal 16.2, to “end abuse, exploitation, trafficking and all forms of violence against and torture of children”.


GOVERNMENT LEGISLATION & REGULATION
PRIVATE SECTOR*
LAW ENFORCEMENT
EDUCATIONAL INSTITUTION
CIVIL SOCIETY
Key Stakeholders in addressing SDG 16.2

*Includes operators, ISPs, content providers, social media & messaging platforms

Source: Broadband Commission – Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online 2019[57]

[56] Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, WeProtect Global Alliance, 2016.

[57] Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online, Broadband Commission, 2019.

< PREVIOUS SECTION NEXT SECTION >

4. Integrating child-centred design:

> **States parties should regulate against known harms and proactively consider emerging research and evidence in the public health sector, to prevent the spread of misinformation and materials and services that may damage children's mental or physical health. Measures may also be needed to prevent unhealthy engagement in digital games or social media, such as regulating against digital design that undermines children's development and rights.**
>
> Source: General comment No. 25 (2021), para 96[58]

Child online safety must be embedded in the design and development of technology. Child-centred design builds child online safety into services and products from the outset. This should include ensuring that child online safety is considered in the regulatory requirements for design and in the licensing of new technologies[59]. Child-centred design may also be referred to as safety/rights/privacy/ethics by design.

Applying the precautionary principle[60] to technology that may impact children and young people ensures that child online safety is considered at an early stage. UNESCO's World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) put forward a 'working definition' of the precautionary principle:

> **"When human activities may lead to morally unacceptable harm that is scientifically plausible but uncertain, actions shall be taken to avoid or diminish that harm.**
>
> Morally unacceptable harm refers to harm to humans or the environment that is:
>
> □ **Threatening to human life or health, or**
>
> □ **Serious and effectively irreversible, or**
>
> □ **Inequitable to present or future generations, or**
>
> □ **Imposed without adequate consideration of the human rights of those affected."[61]**

The precautionary principle should guide a framework for safety and privacy by design to ensure child online safety and children's rights are incorporated in technology at the design stage. Child-centred design should not only be an ethical concept, but a legal requirement.[62] It should also be incorporated into criteria for funding research and development that may affect children's rights online.

Technology and artificial intelligence (AI) have the potential to improve child online safety and to protect children's rights. Support for the development of technological tools to realise children's rights and enhance child online safety is an important aspect of a child online safety policy. The wider impact of AI or other technology designed to protect children must be assessed in light of all children's rights[63] to avoid undermining other rights such as privacy and non-discrimination.

[58] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[59] Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, GOV.UK, 2021.

[60] See Communication from the Commission on the precautionary principle EUR-Lex, 2000; The precautionary principle: Definitions, applications and governance, European Parliament, 2015.

[61] The Precautionary Principle, World Commission on the Ethics of Scientific Knowledge and Technology, 2005.

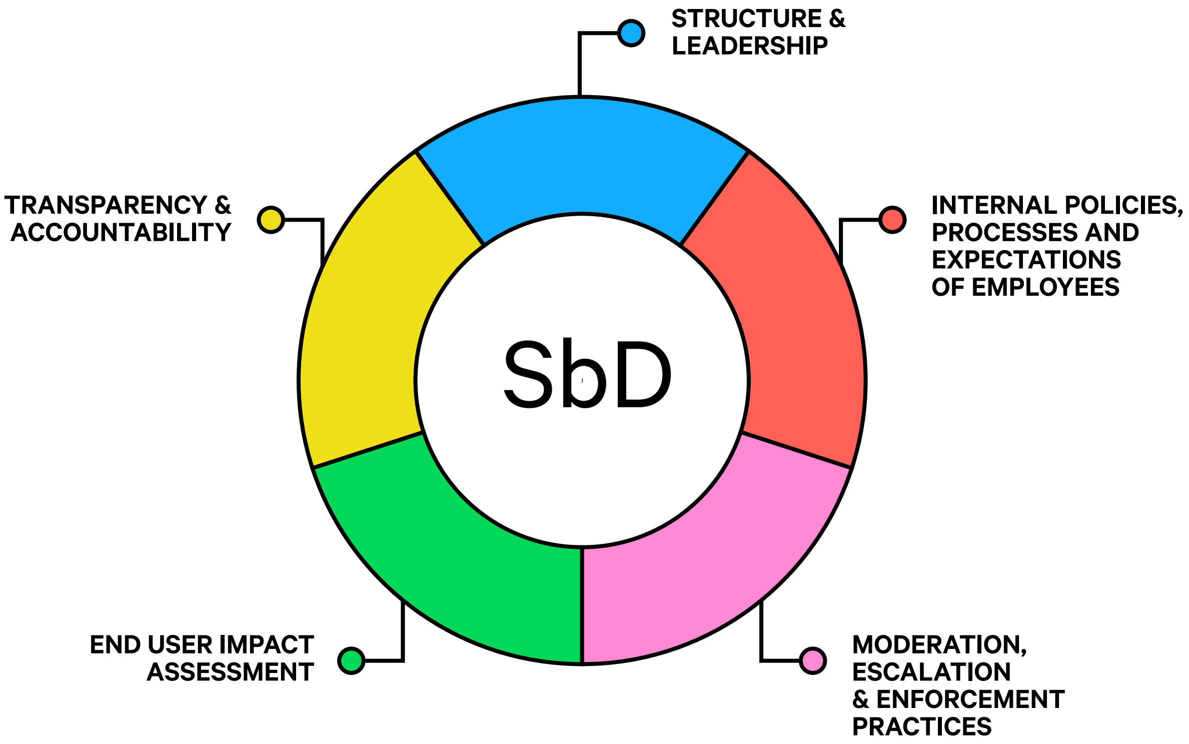
[62] See for example Article 25, General Data Protection Regulation, European Union, 2018.

[63] See for example General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

Children themselves are extremely diverse and the full range of children's characteristics, backgrounds and contexts should be considered in the development, implementation and monitoring of the effectiveness of policies in this area. Effective action on child online safety needs to address perceived tensions. For example, in debates on encryption, advocates for protection from child sexual exploitation and abuse (CSEA) may find their arguments clash with those related to privacy and data protection. Such conflicts must be resolved to the extent that there is a practical outcome, to avoid many years of cyclical debate while children are put at risk or come to harm. In such cases, the 'best interests' of the child should be paramount.[64]

There are several frameworks and processes that support the application of child-centred design in policy making , including the Precautionary Principle, Child Impact Assessments[65] and Consultation with Children.[66] In addition, the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) introduced a standard containing practical steps that companies can follow to design digital products and services that are age appropriate,[67] and the Digital Futures Commission has set out how children's right to play freely could be supported in a digital world by improving the design of digital products and services. Policy makers should always seek to ensure that products and services minimise risk before they are made available to children. Safety by design, and rights by design are systemic in nature and therefore aim to protect millions of children from the outset, not after the fact.


STRUCTURE & LEADERSHIP
TRANSPARENCY & ACCOUNTABILITY
INTERNAL POLICIES, PROCESSES AND EXPECTATIONS OF EMPLOYEES
SbD
END USER IMPACT ASSESSMENT
MODERATION, ESCALATION & ENFORCEMENT PRACTICES

Source: eSafety's Safety by Design[68] initiative Self-Assessment Tools and Principles[69]

[64] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989. (See in particular Article 3, Section 1 on children's rights).

[65] Child Rights Impact Assessment, Digital Futures Commission, 2021.

[66] Child Rights Impact Assessment, Digital Futures Commission, 2021.

[67] IEEE 2089-21 Standard for Age-Appropriate Digital Services Framework, IEEE SA, 2021.

[68] Safety by Design Principles, eSafety Commissioner, 2021.

[69] Safety by Design Principles, eSafety Commissioner, 2021.

< PREVIOUS SECTION NEXT SECTION >

5. Ensuring effectiveness:

> **States parties should mobilise, allocate and utilise public resources to implement legislation, policies and programmes to fully realise children's rights in the digital environment and to improve digital inclusion, which is needed to address the increasing impact of the digital environment on children's lives and to promote the equality of access to, and affordability of, services and connectivity.**
>
> **States parties should ensure that the mandates of national human rights institutions and other appropriate independent institutions cover children's rights in the digital environment and that they are able to receive, investigate and address complaints from children and their representatives. Where independent oversight bodies exist to monitor activities in relation to the digital environment, national human rights institutions should work closely with such bodies on effectively discharging their mandate regarding children's rights.**
>
> Source: General comment No. 25 (2021), paras 28 and 31[70]

Child online safety and children's rights in the digital environment can only be truly effective through practical policy actions, adequate resourcing, and enforcement.

Child online safety is relevant to a wide range of policy areas, including information and communications technology (ICT), education, criminal justice, health, regulation of industry, social and family support, business, human rights and equality, international development, and many others. Cooperation across different ministries and agencies working in policy areas is thus essential for effective action on child online safety. Budgeting in order to resource the policy both within and across different departments will be necessary. A policy with insufficient funds, or a partnership with no capacity, i.e. something which exists only on paper, will not result in effective child online protection.

Understanding effectiveness means reviewing the impact of child online safety policies. Monitoring, evaluation and data collection are key to informing good policy development. Learning from and sharing lessons on effective policy making across borders is an efficient way to maximise effectiveness. Checking the effectiveness of child online safety policy requires consultation not only with the key actors involved, but also with children, to understand how actions are affecting them or could impact on them in the future.[71] It is an ongoing process.

Policy should be data-driven and evidence-based. Both relevant authorities and private companies should be required to collect and share data to aid understanding of child online protection issues, in compliance with data protection laws and principles. Child online safety is a relatively new policy area, so where evidence is not available or contested, policy-makers should take a precautionary approach, or look to other contexts and take a 'what works' approach – for example, with health and safety principles, or frameworks such as INSPIRE: Seven Strategies for Ending Violence Against Children.[72]

Child online safety is not a standalone issue. The effectiveness of child online safety policy will depend on the overall effectiveness of key institutions and their ability to collaborate towards effective protection. Ensuring effective accountability for child online safety overall, and the prevention of CSEA in particular, relies on strong domestic justice systems. The Model National Response (MNR) presents guidance on this issue. Effective approaches to child online safety also rely on adequate resourcing for the institutions that support them, including in areas such as psycho-social support, and regulation in ICT and related fields. Upholding children's rights effectively through child online safety policy depends on efficient human rights legislation and specific legislation and regulation with oversight bodies to guarantee children's rights in both the online and the offline environment.

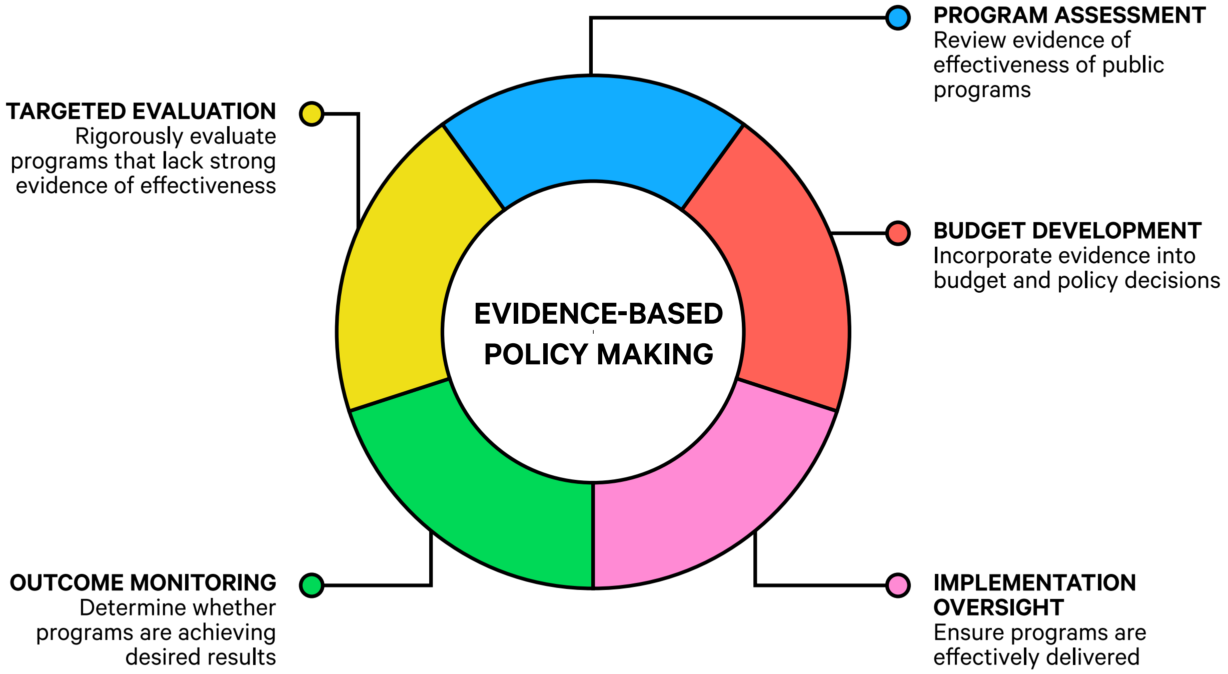
[70] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[71] Digital Futures Commission, 5Rights Foundation, 2021.

[72] INSPIRE Indicator Guidance and Results Framework, World Health Organisation, 2018.

< PREVIOUS SECTION NEXT SECTION >

Policy makers should ensure that the institutional capacity, the resources, and accountability mechanisms are in place to support child online safety policies. Where conflicts arise, the 'best interests' of children should be paramount. Without these, even the best policies will be ineffective.

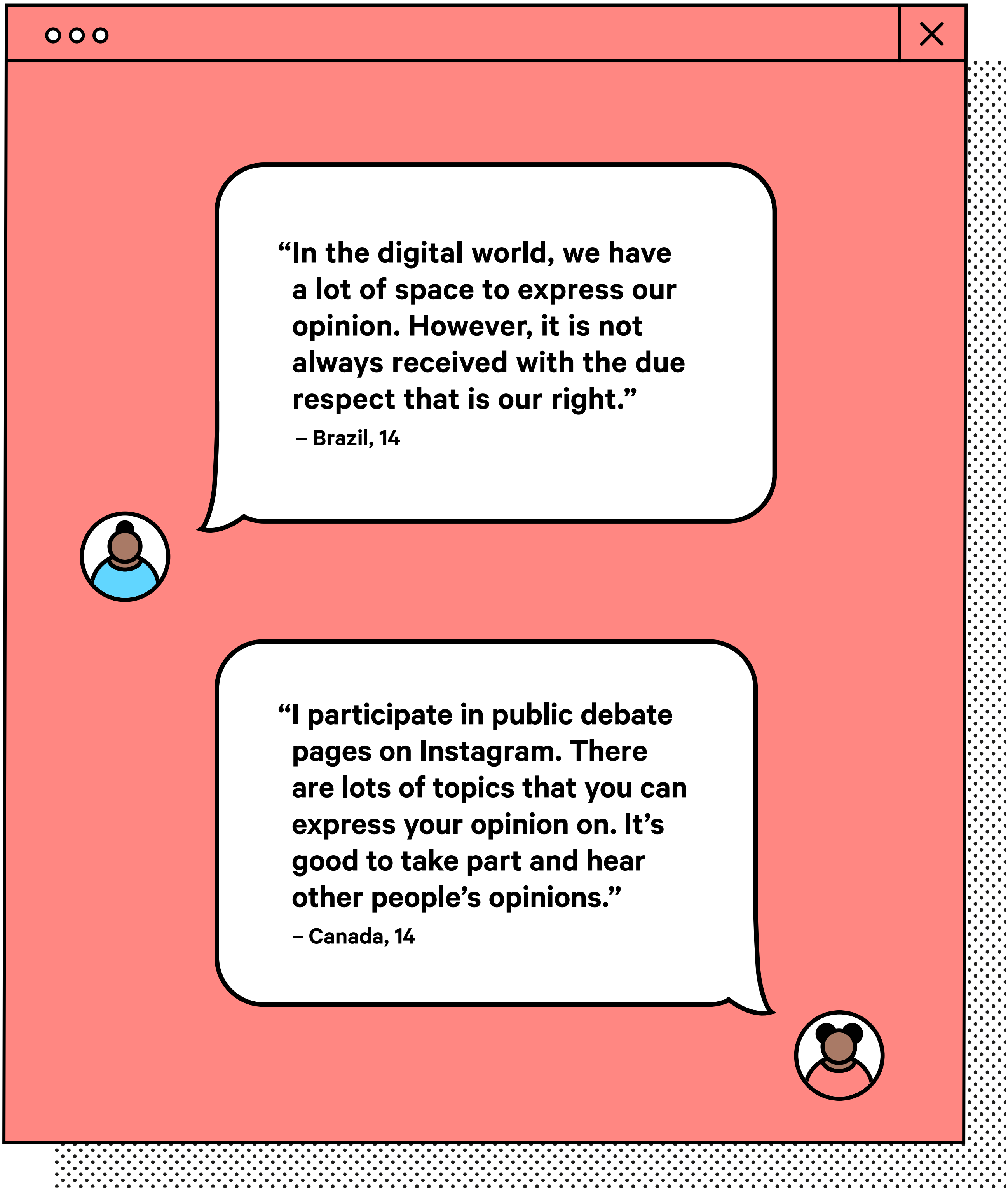

PROGRAM ASSESSMENT
Review evidence of effectiveness of public programs
TARGETED EVALUATION
Rigorously evaluate programs that lack strong evidence of effectiveness
BUDGET DEVELOPMENT
Incorporate evidence into budget and policy decisions
EVIDENCE-BASED POLICY MAKING
OUTCOME MONITORING
Determine whether programs are achieving desired results
IMPLEMENTATION OVERSIGHT
Ensure programs are effectively delivered

Source: Pew Charitable Trusts/MacArthur Foundation: Evidence-Based Policymaking[73]

[73] Evidence-Based Policymaking, MacArthur Foundation, 2014.

< PREVIOUS SECTION

NEXT SECTION >

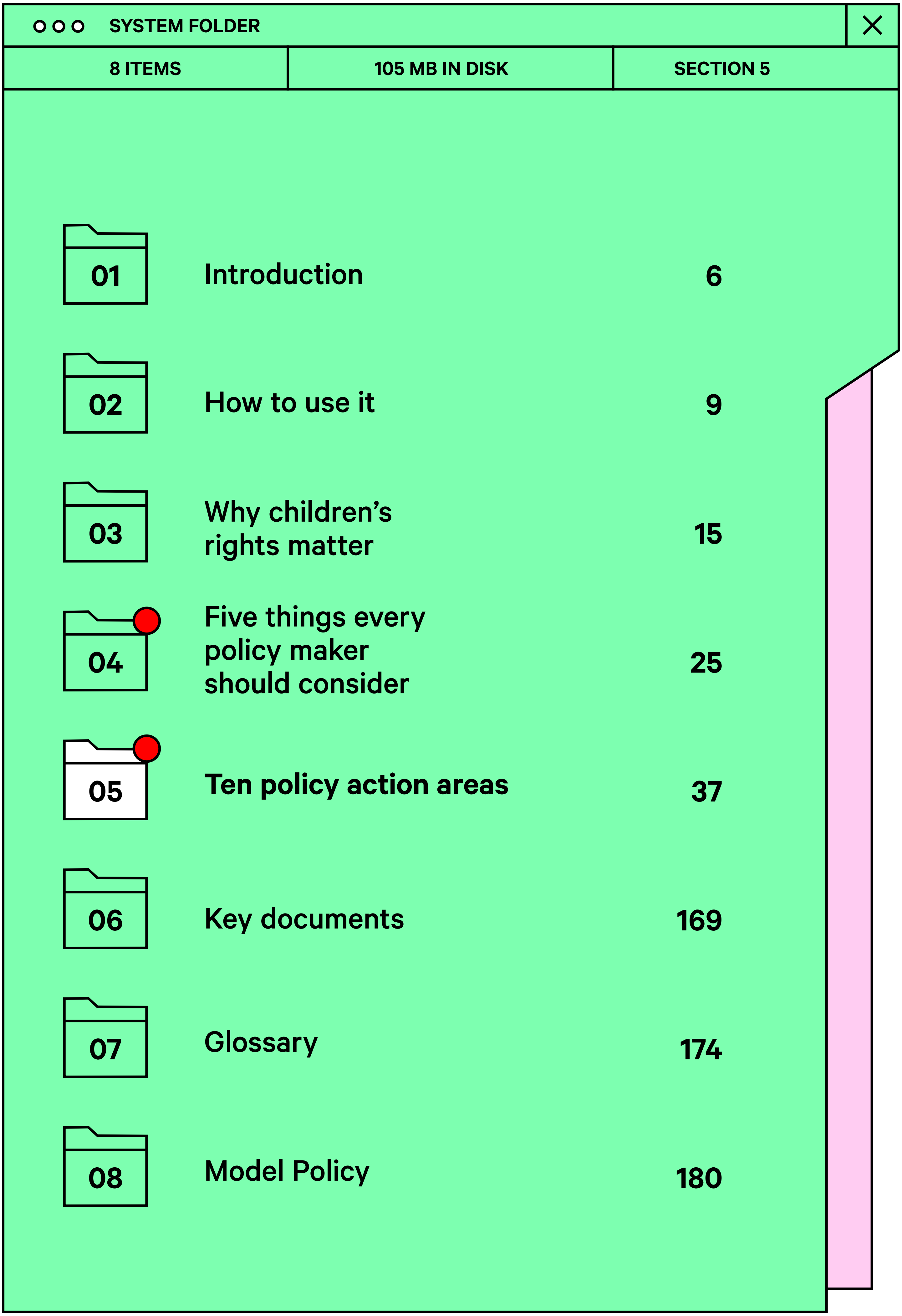


"In the digital world, we have a lot of space to express our opinion. However, it is not always received with the due respect that is our right."

– Brazil, 14

"I participate in public debate pages on Instagram. There are lots of topics that you can express your opinion on. It's good to take part and hear other people's opinions."

– Canada, 14



SYSTEM FOLDER

8 ITEMS | 105 MB IN DISK | SECTION 5

< PREVIOUS SECTION NEXT SECTION >

Ten policy action areas

This section provides model policies that outline the practical actions needed for an effective child online safety policy, and also provides tools for policy makers to design and deliver effective mechanisms which are relevant to their national context.

○ ○ ○ MODEL POLICIES ✕

1. Institutional capacity
2. Legal and regulatory frameworks
3. Personal data, identity and autonomy
4. Response and support systems
5. Corporate responsibility
6. Training
7. Education
8. Public awareness and communications
9. Research and development
10. Global cooperation

Implementation of each of these policy action areas should take into account the four guiding principles on children's rights set out in Chapter 3:

○ ○ ○ PRINCIPLES ✕

- The right to non-discrimination
- The best interests of the child
- The right to life, survival, and development
- The right to be heard

And the five other cross-cutting themes set out in Section A:

○ ○ ○ FIVE THINGS ✕

- Risk and harm
- Accessibility and inclusion
- Chain of responsibility
- Child-centred design
- Effectiveness

< PREVIOUS SECTION NEXT SECTION >

1 Institutional capacity

> **States parties should take legislative and administrative measures to protect children from violence in the digital environment, including the regular review, updating and enforcement of robust legislative, regulatory and institutional frameworks that protect children from recognised and emerging risks of all forms of violence in the digital environment.**
>
> Source: General comment No. 25 (2021), para 82[74]

Objective:

To identify a lead ministry or agency to establish a National Child Online Safety Steering Committee and a stakeholder group of experts to cover all areas of the child online safety policy. To provide adequate resourcing, leadership, and institutional capacity to ensure effective action and cooperation.

Model policy text:

To ensure a holistic approach to child online safety, each of the steps below is necessary.

1a. Affirm public commitment to child online safety at the highest level
National leaders, including the Prime Minister or President, should commit to child online safety on both the national and international stages.

1b. Designate a ministry or agency to take the lead on developing the national child online safety policy
Around the world, a range of different agencies and ministries lead on child online safety policy, and the choice of agency or ministry may affect the way a child online safety policy evolves and prioritises different aspects of child online safety. Child online safety is likely to sit across several ministries, but it is important that a lead agency owns the agenda. In some countries, child online safety policy is led by the ministry responsible for ICT, in others the ministry responsible for children and families, and yet in others, the Ministry of Justice. It may be that where existing groups are working on violence against children (VAC) or cybersecurity, they can be extended to include the necessary expertise in order to prevent siloed working. *The lead agency may be chosen for its authority, expertise, resources, capacity or enthusiasm – but any lead agency will have to work with others.* Whichever ministry takes the lead, it must commit to a holistic approach that reflects the overarching needs of child online safety.

1c. Publish a definitions and language manual
The designated lead ministry should publish a full list of definitions and language that reflects definitions used in international best practice.[75] ▶

[74] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[75] See for example, Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International, 2016.

< PREVIOUS SECTION NEXT SECTION >

1d. Establish a National Child Online Safety Steering Committee
The National Child Online Safety Steering Committee will be responsible for policy implementation and development and will serve as a focal point for national and regional cooperation. It will be responsible for taking the Child Online Safety Toolkit and developing the strategy to implement it – this might be called the action plan. The Committee will address a broad set of competencies that cover various policy areas, including education, health, justice, consumer protection, data protection, law enforcement, ICT, and family and children's services, among others, and will supervise implementation and uphold standards. The Committee should be formally required to cooperate with all those who have a remit for child safety or cybersecurity, and should report regularly to the lead ministry.

1e. Understanding child online safety stakeholders
The enforcement community, business, third sector, children's rights organisations, educational institutions, parents/carers and academia all hold useful insights and important interests in child online safety. In some contexts, creating a stakeholder group may be useful to support the Committee with its activities and ground its action plan in real-life scenarios. In other contexts, informal discussions or calls for evidence from an open network of stakeholders may be more effective. Either way, the National Child Online Safety Steering Committee should seek to engage with key stakeholders who can support their activities. Interagency cooperation should be promoted. The purpose of stakeholder engagement is to focus on implementation, not policy development.

1f. Define roles and responsibilities of stakeholders
There should be a co-regulatory framework that defines the roles and responsibilities of all organisations developing and managing digital infrastructure, networks and services, and the duties of government departments. Minimum standards should be established for all in the value chain, including those responsible for infrastructure, hardware, and digital products and services, and those who manage or use them when they interact with children. These standards should focus on child safety and the full realisation of children's rights in the digital world. Civil society participation and child consultation should be ensured in stakeholder groups.

1g. Define performance indicators and evaluation
Each aspect of the implementation plan should have a corresponding accountable authority (person, institution, body) and human and financial resources to successfully complete the task envisioned. It may be that the same authority is responsible for more than one policy area, or a single area of expertise. Key Performance Indicators (KPIs), evaluation mechanisms and clear reporting structures should be introduced to enable the Steering Committee to oversee and manage progress. As the digital environment evolves rapidly, KPIs will require constant review.

1h. Ensure integration of child online safety across government policy areas
Any relevant national plans, such as a National Broadband Plan or digital literacy framework, should include child online safety policy as part of the rollout strategy. Plans that take place over several years should be checked at key milestones.

< PREVIOUS SECTION NEXT SECTION >

Roadmap to achieving the policy:

A Affirm public commitment to child online safety at the highest level

National leaders, for example, Prime Minister, President or Ministers, should commit to child online safety on both the national and the international stage.

If yes, provide details:

If no, it will help to make a plan, fully evidenced with a broad group of supporters and take to national leaders - your plan will:

1. Set out the rationale with relevant evidence and data; if data is not available for your country, use international data.
2. Identify key decision makers and target evidence-based advocacy efforts to establish their understanding and commitments.
3. Identify and engage with advocates and experts (internal, local and international) to support your case.
4. Review the status of national efforts and policies addressing child online safety and other forms of violence against children (VAC), in addition to women and girls (VAWG), and cybersecurity.
5. Based on the above, agree (in consultation with key stakeholders) how to deliver a holistic child online safety policy that includes and builds on existing programmes.
6. Identify existing duties and obligations in line with existing frameworks and other relevant national plans of action and cross-sector committees (e.g. VAC, VAWG, cybersecurity).
7. In consultation with key stakeholders, create a plan of action: costed, timed and with a leading agency and a named person or organisation responsible for each action.
8. Take your roadmap to the decision makers with the fullest support, to get their consent and sign off.

< PREVIOUS SECTION NEXT SECTION >

1 Institutional capacity

B Designate a ministry or agency to take the lead on developing the national child online safety policy

Around the world, a range of different agencies and ministries lead on child online safety policy, and the choice of agency or ministry may affect the way a child online safety policy evolves and prioritises different aspects. Child online safety is likely to sit across several ministries, but it is important that a lead agency owns the agenda. In some countries, child online safety policy is led by the ministry responsible for ICT, in others the ministry responsible for children and families, and in yet others, the Ministry of Justice. The lead agency may be chosen for its authority, expertise, resources, capacity or enthusiasm – but any lead agency will have to work with others. Whichever ministry takes the lead, it must commit to a holistic approach that reflects the overarching needs of child online safety.

If yes, provide details:

If no, it will help to use the SWOT tool. See Supportive tools 1 (page no. 47) to choose a lead ministry or agency.

C Publish a definitions and language manual

The designated lead ministry should publish a full list of definitions and language, that reflects definitions used in international best practice.[76]

If yes, check it is in line with the definitions in the glossary and definitions (page no. 178) to ensure effective translation.

If no, it will help to refer to the glossary and definitions (page no. 178) as best practice to ensure effective translation.

[76] See for example Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International, 2016.

< PREVIOUS SECTION NEXT SECTION >

D National Child Online Safety Steering Committee

The National Child Online Safety Steering Committee will be responsible for policy development and implementation, and will serve as a focal point for regional and national cooperation. It will develop the strategy to deliver the Child Online Safety Toolkit. The Committee will address a broad set of competencies that cover various policy areas, including education, health, justice, consumer protection, data protection, law enforcement, ICT, and family and children's services, among others, and will supervise implementation and uphold standards. The Committee should report to the lead ministry.

If yes, provide details:

If no, it will help to:

1. Consider which ministries and government organisations can contribute to the effective delivery of the child online safety policy and engage in regular meetings.
2. Consider regional or local representation that may have a stake in child online safety.
3. Involve leading experts to ensure that plans are considered best practice and are fit for purpose.
4. Draw on evidence from business and civil society.

< PREVIOUS SECTION NEXT SECTION >

E Understanding child online safety stakeholders

It may be useful to bring together stakeholders in a group with a formal role of supporting and informing the Steering Committee. Alternatively, it may be more practical to engage with stakeholders on a more informal or 'as needed' basis. In all events, it is likely that there will be a wide group of 'interested parties', including parents/carers, teachers and children, and a smaller group of people with relevant skills and expertise – for example, the enforcement community, industry, child rights experts, NGOs (both national and international), health professionals, and academics. Making use of their interest and expertise can be very beneficial for advocating or implementing child online safety policies in multiple contexts.

If yes, provide details:

If no, it will help to:

1. Make a list of stakeholders, skills and expertise, that cover the policy areas listed in the toolkit. For prompts, see the template provided as Supportive tools 2 (page no. 49).
2. Ensure that they include children, or representatives who work directly with children.
3. If a formal group, set out terms of reference that clearly commit the stakeholder group to the activities of the Steering Committee.

< PREVIOUS SECTION

NEXT SECTION >

F Define roles and responsibilities

There should be a co-regulatory framework that defines the roles and responsibilities of all organisations developing and managing digital infrastructure, networks and services, and the duties of government departments. Minimum standards should be established for all in the value chain, including those responsible for infrastructure, hardware, and digital products and services, and those who manage or use them when they interact with children. These standards should focus on child safety and the full realisation of children's rights in the digital world. Civil society participation should be ensured in stakeholder groups.

If yes, provide details:

If no, it will help to:

1. Establish a clear line of responsibility for each of the actions in your plan.
2. Map multiple agencies, government, regulatory or designated organisations, schools, charities, health institutions and businesses with responsibilities to ensure that all aspects are covered, transparent and accountable.

G Define performance indicators and evaluation

Each aspect of the implementation plan should have a corresponding accountable authority (person, institution, body) and human and financial resources to successfully complete the task envisioned. It may be that the same authority is responsible for more than one policy area, or a single area of expertise. Key Performance Indicators (KPIs), evaluation mechanisms and clear reporting structures should be introduced to enable the Steering Committee to oversee and manage progress. As the digital environment evolves rapidly, KPIs will require constant review.

If yes, provide details:

If no, it will help to:

1. Establish KPIs and review processes as part of the strategic plan. For example, the KPIs laid out in Child Online Protection in Rwanda.[77]
2. Establish clear lines of responsibility to the Steering Committee.

[77] Child Online Protection in Rwanda, 5Rights Foundation, 2019.

< PREVIOUS SECTION NEXT SECTION >

H Ensure integration of child online safety across government policy areas

Any relevant national plans – such as a National Broadband Plan, National Plan of Action on Violence Against Children (VAC), digital literacy framework, cybersecurity strategy, etc – should include child online safety policy as part of the rollout strategy. Plans that take place over several years should be reviewed and updated at key milestones.

If yes, provide details:

If no, it will help to:

1. Use the checklist provided in Supportive tools 3 to review policy areas and identify if child online safety is included (page no. 51). It may help to appoint an external expert to check the strategic plan against existing government policy and provision.
2. Bring anomalies to the National Child Online Safety Steering Committee, created in process D.

How this aligns with foundational documents:

> **Governments should put in place a national coordinating framework with a clear mandate and sufficient authority to coordinate all activities related to children's rights and digital media and ICTs at cross-sectoral, national, regional, and local levels. Governments should include time-bound goals and a transparent process to evaluate and monitor progress and must ensure that the necessary human, technical and financial resources are made available for the effective operation of this framework.**
>
> **Governments should establish a multi-stakeholder platform to steer the development, implementation and monitoring of the national digital agenda for children. Such a platform should bring together representatives of the most important constituencies, including: children and young people; associations of parents/caregivers; the relevant sections of government; the education, justice, health and social care sectors; national human rights institutions and relevant regulatory bodies; civil society; industry; academia; and relevant professional associations.**
>
> Source: ITU: Guidelines for policy-makers on Child Online Protection 2020[78]

[78] Guidelines for policy-makers on Child Online Protection, International Telecommunication Union, 2020.

< PREVIOUS SECTION NEXT SECTION >

Supportive tools:

1. SWOT template to identify the most appropriate lead department or ministry

Process B ('Designate a ministry or agency to take the lead on developing the national child online safety policy') requires you to carefully identify your most appropriate lead agency for child online safety. This tool is designed to support you in this process.

Many countries have taken different approaches in choosing a lead agency – for example:

- **Tanzania** – Ministry for Health
- **Ghana** – Ministry for Communications
- **Ethiopia** – Regulatory Authority
- **Australia** – Department of Infrastructure, Transport, Regional Development and Communications
- **UK** – Department for Digital, Culture, Media and Sport

To help you select the right ministry or department, complete a SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) of each potential ministry or department to identify which is best placed to take the lead on child online safety:

Strengths	Weaknesses
Things to consider: does this ministry have any particular strengths with online safety? Are any of the policy action areas already in the remit of the ministry? Are they resourced well enough to take on lead responsibilities? Are they connected and influential enough to do the job? Is their leadership willing and able to take on the brief?	**Things to consider:** does this ministry have any particular weaknesses regarding online safety? Do they lack capacity or capability to take on any additional remits? Do they lack the connections or influence needed to deliver on this cross-cutting brief? Is leadership lacking or not interested in the brief?
Opportunities	**Threats**
Things to consider: are there any synergies between the child online safety brief and emerging policy briefs in this ministry (e.g. broadband or 5G rollout)? Is this ministry staffed by civil servants or led by politicians that are potentially more effective than others?	**Things to consider:** is the ministry already under-performing in existing briefs? Are there any looming threats to the ministry (e.g. expected budget cuts)? Does the ministry have any competing interests that may present challenges to them taking the lead (e.g. conflicting funding or agreements in place with telecom providers or tech companies)? Is the leadership 'on the way out'?

< PREVIOUS SECTION NEXT SECTION >

2. Template to identify stakeholders

This template helps you list the stakeholders needed to create a stakeholder group, with relevant roles and responsibilities, as required by Process E ('Understanding child online safety stakeholders'). The representatives, organisations and roles and responsibilities will depend on the local context, and there may be several for each type. Once you have identified the right ministry or organisation to lead, it will also be important to include the same or similar stakeholders in the process to ensure balance, efficiency and proper delivery.

The types listed below reflect those in the ITU Guidelines for policy-makers on Child Online Protection 2020 and those mentioned in General comment No. 25 (2021).

Stakeholder representative	Type	Organisation	Role and responsibilities
Example: Named individual or representative with suitable authority to contribute/make decisions/ensure allocation of resources	Children and young people	Youth Group X	The child's voice: to provide insights from children's perspective; to highlight children's concerns and questions
✎	5Rights youth advisory group		The child's voice: to provide insights from children's perspective; to highlight children's concerns and questions
	Parents, carers, educators		To ensure that policies support adults with caring duties
	Industry		To ensure policies create obligations for all products and services to be child-centred and safe
	Research community and NGOs		To ensure policies reflect current evidence and expertise

▶

< PREVIOUS SECTION NEXT SECTION >

1 Institutional capacity

Stakeholder representative	Type	Organisation	Role and responsibilities
	Law enforcement		To ensure policies are enforceable and to educate the enforcement community
	Social services		To ensure that policies consider vulnerable children
	Healthcare services		To reflect medical advice and e-victim support, and/or support for those at risk or harmed
	Government ministries and regulators		To involve specialist regulators and ministries who are not the lead ministry
	Broadband, mobile and WIFI network operators		To support safe and affordable digital access for children
	Children's rights organisations		To ensure the full gamut of children's rights are enabled and realised in digital policies
	Academics, lawyers, individuals, organisations with a particular expertise, for example in law, algorithmic audit, moderation practices, etc.		To provide specialist help on an 'as needed' basis, to ensure that policies are sophisticated but also practical

< PREVIOUS SECTION NEXT SECTION >

1 Institutional capacity

3. Checklist to identify which policy areas address child online safety

This checklist helps guide you through a review of relevant existing policies to establish whether each contains a child online safety aspect. This helps you to achieve Process H (‘Ensure integration of child online safety across government policy areas’).

Please notify the child online safety stakeholder group of the findings of this review.

Child online safety element reflected in child online safety policy	Tick if already included	If not, identify gaps and anomalies, and recommended changes, and report to the child online safety stakeholder group
National Broadband Plan	□	
Sustainable Development Goals implementation frameworks and roadmaps	□	
All necessary education and training curricula	□	
Digital literacy frameworks for children	□	
National educational curriculum for schools	□	
Teacher and social worker vocational curriculum	□	
Police and law enforcement vocational curriculum	□	

< PREVIOUS SECTION

NEXT SECTION >

1 Institutional capacity

Child online safety element reflected in child online safety policy	Tick if already included	If not, identify gaps and anomalies, and recommended changes, and report to the child online safety stakeholder group
Consumer rights	□	
Violence against children, child protection and safeguarding strategy	□	
Criminal justice	□	
Human rights	□	
Children's rights	□	
Equalities and anti-discrimination	□	
Data protection	□	
International trade	□	
Gambling controls	□	

▶

< PREVIOUS SECTION NEXT SECTION >

1 Institutional capacity

Child online safety element reflected in child online safety policy	Tick if already included	If not, identify gaps and anomalies, and recommended changes, and report to the child online safety stakeholder group
Advertising standards	□	
Financial crimes	□	
Education	□	
Health	□	
International cooperation	□	
Others	□	

< PREVIOUS SECTION
NEXT SECTION >

Other resources for reference:

1. **The UK Council for Internet Safety (UKCIS) as a model for a child online safety stakeholder group**[79]

   The UK Council for Internet Safety (UKCIS) is a collaborative forum through which the government, the tech community and the third sector all work together. UKCIS is part of the Department for Digital, Culture, Media & Sport, the Department for Education and the Home Office. Over time, UKCIS has been a meeting place for business, academia, child safety experts, civil servants, and ministers. It has also commissioned important research which has provided an evidence base for policy. By contrast with the Toolkit recommendation, UKCIS was not formally attached to a plan of action for a steering group.

2. **The ITU Guide to developing a national cybersecurity strategy – strategic engagement in cybersecurity**[80]

   Facilitated by ITU, twelve partners from the public and private sectors, academia and civil society share their experience, knowledge and expertise, providing an aggregated, harmonised set of principles on the development, establishment and implementation of national cybersecurity strategies. The guide's objective is to instigate strategic thinking and help national leaders and policy makers to develop, establish and implement national cybersecurity strategies worldwide.

3. **The Council of Europe Handbook for Policy Makers on the Rights of Children in the Digital Environment**[81]

   This handbook aims to support Council of Europe Member States in implementing Recommendation CM/Rec(2018)7 and the guidelines to respect, protect and fulfil the rights of the child in the digital environment. This document includes the world's first comprehensive guidelines for States regarding children's rights in the digital environment.

4. **Child Online Protection in Rwanda**[82]

   Created in partnership between 5Rights Foundation, University of East London, University of Rwanda and the Government of Rwanda, the Child Online Protection Policy offers a high-level implementation plan as an exemplar for any nation considering child online protection.

[79] UK Council for Internet Safety, Department for Digital Culture, Media & Sport, Department for Education & Home Office, 2021.

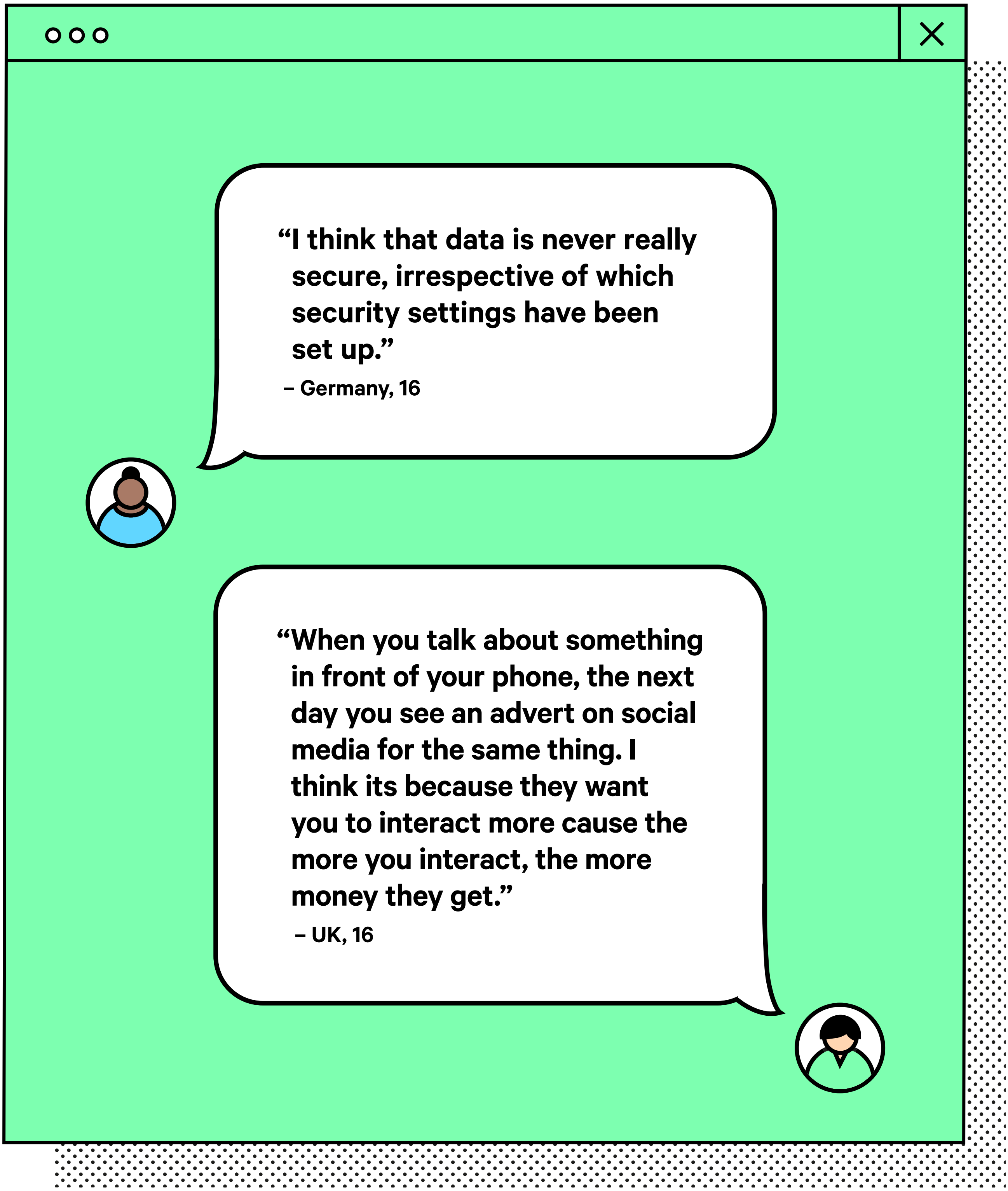
[80] Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity, International Telecommunication Union, 2018.

[81] Handbook for policy makers on the rights of the child in the digital environment, Council of Europe, 2020.

[82] Child Online Protection in Rwanda, 5Rights Foundation, 2019.

< PREVIOUS SECTION

NEXT SECTION >



"I think that data is never really secure, irrespective of which security settings have been set up."

– Germany, 16

"When you talk about something in front of your phone, the next day you see an advert on social media for the same thing. I think its because they want you to interact more cause the more you interact, the more money they get."

– UK, 16

< PREVIOUS SECTION NEXT SECTION >

2 Legal and regulatory frameworks

> **Children may face particular difficulties in obtaining remedy when their rights have been abused in the digital environment by business enterprises, in particular in the context of their global operations. States parties should consider measures to respect, protect and fulfil children's rights in the context of businesses' extraterritorial activities and operations, provided that there is a reasonable link between the State and the conduct concerned. They should ensure that businesses provide effective complaint mechanisms; such mechanisms should not, however, prevent children from gaining access to State-based remedies. They should also ensure that agencies with oversight powers relevant to children's rights, such as those relating to health and safety, data protection and consumer rights, education and advertising and marketing, investigate complaints and provide adequate remedies for violations or abuses of children's rights in the digital environment.**
>
> Source: General comment No. 25 (2021), para 48[83]

Objective:

To strengthen and re-align the domestic legal and regulatory regimes related to child online safety, and to strengthen the capacity and capability of law enforcement agencies and regulatory bodies in the child online safety field including their capacity to collaborate with other sectors, in particular the ICT sector.

Model policy text:

To ensure a holistic approach to child online safety, each of the steps below is necessary.

2a. Strengthen and enforce laws that prohibit child online safety-related offences
Criminal laws and procedures facilitate the investigation and prosecution of online offences that violate children's right to protection and should be strengthened and amended in line with international standards and best practices. This should include the introduction of mandatory risk assessments to reduce potential for harm, enhancing sanctions and sentencing frameworks where necessary. It should also include the potential for notice and takedown procedures. Criminal laws concerning child online safety should be developed in light of all children's rights, including their right to be heard and to participation.[84]

2b. Introduce data protection regulations and independent supervisory authorities, ensuring that children's data is protected appropriately, and collected only where necessary with high levels of security and care
Such general regulations should include special category status for children's data, requiring higher levels of protection and safeguards by default as well as protections against the inappropriate commercial use of children's data. Where consent is sought from children, or parents/carers on their behalf, for the online collection and processing of younger children's data it must be informed and meaningful. Data gathering for safeguarding purposes should be given special consideration in exceptional circumstances where this is in the best interests of the child.

[83] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[84] For example, legal frameworks that do not make it clear whether self-generated sexual images that are exchanged on consensual basis between children will be considered illegal Child Sexual Abuse Material. Even if children are not prosecuted in practice this legal uncertainty with potential criminalisation may undermine trust, control and autonomy rights.

< PREVIOUS SECTION NEXT SECTION >

2c. Strengthen criminal investigation, prosecution and sentencing for online child sexual exploitation or abuse[85]

Criminal justice agencies with responsibilities for child online safety-related offences should be trained in child online safety issues with the aim of driving greater prevention, successful prosecution and appropriate sentencing as well as greater understanding of the impact on victims. The capabilities of relevant investigation and response teams should be reviewed and strengthened to detect, prevent and respond to cybersecurity threats, specifically those related to child online safety. Criminal justice systems should be able to ensure timely access to justice.

2d. Review and strengthen youth justice systems

Ensure that the law is clear and proportionate to minimise the risk of children coming into conflict with the law in the context of child online safety. Where children face criminal sanctions related to child online safety, for example in relation to cyberbullying or image-based sexual abuse, the justice system must make every effort to prevent children from being criminalised and provide adequate support and legal representation to those children who come into conflict with the law to protect their rights.

2e. Identify and ratify child online safety-related international treaties & protocols

Building a sustainable ecosystem of child online safety requires a multi-stakeholder approach and participation on a global scale. Each country should identify and ratify relevant international and regional protocols and treaties and take steps to implement their measures.

2f. Strengthen the capacity of law enforcement agencies

Shortcomings in enforcement and the judiciary will be identified, and measures will be put in place to increase awareness, reporting and successful prosecution. International training and skills sharing should be sought where possible, and cross-sector coordination and collaboration between industry and law enforcement should be encouraged.

[85] Child sexual exploitation and abuse (CSEA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline.

< PREVIOUS SECTION NEXT SECTION >

Roadmap to achieving the policy:

A Strengthen and enforce laws that prohibit child online safety-related offences

Criminal laws and procedures facilitate the investigation and prosecution of online offences that violate children's right to protection and should be strengthened and amended in line with international standards and best practices. This should include the introduction of mandatory risk assessments to reduce the potential for harm and enhancing sanctions and sentencing frameworks where necessary. It should also include the potential for notice and takedown procedures. Criminal laws concerning child online safety should be developed in light of all children's rights, including their right to be heard and to participation.[86]

If yes, provide details:

If no, it will help to:

1. Identify relevant laws. For prompts, see the checklist provided as Supportive tools 1 (page no. 64).
2. Check against international standards in each of the areas - i.e. youth justice etc.
3. Carry out risk assessments on existing laws.
4. Commission gap analysis from experts.
5. Propose amendments to existing laws.
6. Plan advocacy efforts to ensure amendments are adopted and their implementation is appropriately resourced.

[86] For example, legal frameworks that do not make it clear whether self-generated sexual images that are exchanged on consensual basis between children will be considered illegal Child Sexual Abuse Material. Even if children are not prosecuted in practice this legal uncertainty with potential criminalisation may undermine trust, control and autonomy rights.

< PREVIOUS SECTION NEXT SECTION >

B Introduce data protection regulations and independent supervisory authorities, ensuring that children's data is protected appropriately, and collected only where necessary with high levels of security and care

Some jurisdictions have general data protection legislation that may need enhancing or formalising, in order to ensure that children are offered age-appropriate protections. In others, where no or little data protection is in place, it may be necessary to put forward data protection legislation exclusively for children. In both cases, children's data must be considered a special category, requiring higher levels of protection and safeguards by default, as well as protections against the inappropriate commercial use of children's data. Where consent is sought from children, or parents/carers on their behalf, the online collection and processing of younger children's data must be informed and meaningful. Data gathering for safeguarding purposes should be given special consideration in exceptional circumstances, where this is in the best interests of the child.

If yes, provide details:

If no, it will help to:

1. Conduct gap analysis of existing regulatory frameworks on data protection.
2. Propose new regulations or amendments with resources and evidence to support them.
3. Establish or resource existing independent supervisory authorities to monitor and ensure compliance.
4. Align data protection for children with existing international practice.

< PREVIOUS SECTION

NEXT SECTION >

C Strengthen criminal investigation, prosecution and sentencing for online child sexual exploitation or abuse[87]

Criminal justice agencies with responsibilities for child online safety-related offences should be trained in child online safety issues, with the aim of driving greater prevention, successful prosecution and appropriate sentencing, as well as a greater understanding of the impact on victims. The capabilities of relevant investigation and response teams should be reviewed and strengthened to detect, prevent and respond to cyber threats or abuse related to child online safety. Criminal justice systems should be able to ensure timely access to justice.

If yes, provide details:

If no, it will help to:

1. Incorporate child online safety into the curriculum (see Policy action area on Training for guidance and resources page no. 144).
2. Review skills and gaps relating to child online safety.
3. Review resources to ensure effective access to child-centred justice.

[87] Child sexual exploitation and abuse (CSEA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline.

< PREVIOUS SECTION NEXT SECTION >

D Review and strengthen youth justice systems

Ensure that the law is clear and proportionate in order to minimise the risk of children coming into conflict with the law in the context of child online safety. Where children face criminal sanctions related to child online safety, for example in relation to cyberbullying or image-based sexual abuse, the justice system must take every effort to prevent children being criminalised and provide adequate support and legal representation to those children who come into conflict with the law to protect their rights.

If yes, provide details:

If no, it will help to:

1. Conduct a review and gap analysis of the youth justice system.
2. Propose amendments where needed.
3. Undertake capacity building of key professionals and consider prevention and awareness raising strategies to reduce the risks of criminalisation.

E Identify and ratify child online safety-related international treaties and protocols

Building a sustainable ecosystem of child online safety requires a multi-stakeholder approach and participation on a global scale. Each country should identify and ratify relevant international and regional protocols and treaties and take steps to implement their measures.

If yes, provide details:

If no, it will help to:

1. Check resources in Annexe D.
2. List relevant instruments.
3. Identify any barriers to ratification.
4. Draw up proposals for signature and ratification.
5. Sign and ratify.

< PREVIOUS SECTION NEXT SECTION >

F Strengthen the capacity of law enforcement agencies

Shortcomings in enforcement and the judiciary should be identified, and measures will be put in place to increase awareness, reporting and successful prosecution. International training and skills sharing should be sought where possible, and cross-sector coordination and collaboration between industry and law enforcement should be encouraged.

If yes, provide details:

If no, it will help to:

1. Identify skills gaps
2. Identify training modules (see Policy action area on Training for guidance and resources, page no. 144).
3. Identify possible national and international partners for skills sharing (see Policy action on Global cooperation for resources, page no. 161).

How this aligns with foundational documents:

> **"Legislation and regulation are essential instruments for ensuring that the activities and operations of business enterprises do not adversely impact on or violate the rights of the child. States should enact legislation that gives effect to the rights of the child by third parties and provides a clear and predictable legal and regulatory environment which enables business enterprises to respect children's rights."**
>
> Source: General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, para 53[88]

> **Notwithstanding the existence of internal grievance mechanisms, governments should establish monitoring mechanisms for the investigation and redress of children's rights violations, with a view to improving accountability of ICT and other relevant companies, as well as strengthen regulatory agency responsibility for the development of standards relevant to children's rights and ICTs. This is especially important because other remedies available to those adversely affected by corporate action – such as civil proceedings and other judicial redress – are often cumbersome and expensive.**
>
> Source: ITU Guidelines for policy-makers on Child Online Protection 2020[89]

[88] General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, UNCRC, 2013.

[89] Guidelines for policy-makers on Child Online Protection, International Telecommunication Union, 2020.

< PREVIOUS SECTION NEXT SECTION >

Supportive tools:

1. A legal checklist: An example

This is designed to help you identify relevant laws and policies in your jurisdiction as part of achieving Process A ('Strengthen and enforce laws that prohibit child online safety-related offences'). The UK examples are indicative and should be replaced with relevant national or regional examples.

Policy area	Law/regulation	Status	Does it include child online safety?	Regulator/ court
Consumer rights	Consumer Rights Act 2015[90] Toy (Safety) Regulations 2011[91] General Product Safety Regulations 2005[92]	Law Statutory Instrument Statutory Instrument	Yes	Court
Child protection	Children and Social Work Act 2017[93] Children Act 2004[94] Digital Economy Act 2017[95]	Law Law Law	Yes	Family court
Criminal justice	Various offences through criminal legislation	Law	Yes	Court
Human rights including children's rights	Human Rights Act 1998[96] UN Convention on the Rights of the Child[97] General comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment[98]	Law Treaty Treaty	Yes	Court Equality and Human Rights Commission (and national Commissions) Reporting to UN Committee on the Rights of the Child UN Courts

[90] Consumer Rights Act 2015, Chapter 3 Digital Content, UK; Consumer Rights Act (Digital Content) Guidance for Business, Department for Business Innovation and Skills, 2015.

[91] Toy (Safety) Regulations 2011, Office for Product Safety & Standard, 2011.

[92] General Product Safety Regulations 2005, UK Gov, 2017.

[93] Children and Social Work Act 2017, Chapter 2 Safeguarding Children, UK Gov, 2004.

[94] Children Act 2004, UK Gov, 2004.

[95] Digital Economy Act 2017, UK Gov, 2017.

[96] Human Rights Act 1998, UK Gov, 1998.

[97] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989.

[98] General comment No. 25 (2021) on children's rights in relation to the digital environment, United Nations Committee on the Rights of the Child, 2021.

< PREVIOUS SECTION NEXT SECTION >

2 Legal and regulatory frameworks

Policy area	Law/regulation	Status	Does it include child online safety?	Regulator/ court
Data protection	Age Appropriate Design Code 2020[99] Data Protection Act 2018[100]	Law Law	Yes	Information Commissioner's Office
International trade	Trade Act 2021[101] (adds a child protection clause)	Law	Yes	Court
Gambling	Gambling Act 2005[102]	Law	Yes	Gambling Commission
Advertising	Advertising Standards Authority, CAP Code 2010[103] Advertising Standards Authority, BCAP Code 2010[104]	Voluntary Voluntary	Yes	Membership organisation with co-regulation under the auspices of Ofcom
Financial crimes	Fraud Act 2006[105] Theft Act 1968[106] Proceeds of Crime Act 2002[107] Money Laundering, Terrorist Financing and Transfer of Funds (Information of the Payer) Regulations 2017[108] Sanctions and Anti-Money Laundering Act 2018[109]	Law Law Law Law Law	No, but there is a voluntary code of conduct from credit card companies on CSEA and pornography	Court Court Court Court & Financial Services Authority Court & Financial Services Authority
Education	Children and Social Work Act 2017[110] UN Convention on the Rights of the Child[111] General comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment[112]	Law Treaty Treaty	Yes	Court, Ofsted Reporting to UN Committee on the Rights of the Child

[99] Age appropriate design code 2020, UK Gov, 2020.
[100] Data Protection Act 2018, UK Gov, 2018.
[101] Trade Act 2021, UK Gov, 2021.
[102] See Gambling Act 2005 Part 1, Section 4 (Remote gambling) and Part 4 (Protection of children and young persons) 2005, UK Gov, 2005.
[103] See Advertising Standards Authority Non Broadcast CAP Code Section 5 (Children), Advertising Standards Authority, 2010.
[104] See Advertising Standards Authority Broadcast BCAP Code Section 5 (Children), Advertising Standards Authority, 2010.
[105] Fraud Act 2006, UK Gov, 2006.
[106] Theft Act 1968, UK Gov, 1968.
[107] Proceeds of Crime Act 2002, UK Gov, 2002.
[108] Money Laundering, Terrorist Financing and Transfer of Funds (Information of the Payer) Regulations 2017, UK Gov, 2017.
[109] Sanctions an Anti-Money Laundering Act 2018, UK Gov, 2018.
[110] Children and Social Work Act 2017, UK Gov, 2017 (especially Chapter 4 on Relationships, sex and PSHE education).
[111] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989.
[112] General comment No. 25 (2021) on children's rights in relation to the digital environment, United Nations Committee on the Rights of the Child, 2021.

< PREVIOUS SECTION NEXT SECTION >

Policy area	Law/regulation	Status	Does it include child online safety?	Regulator/ court
Health	Health and Social Care Act 2012[113]	Law	No	Chief Medical Officer Court Family Court
International cooperation	Sustainable Development Goals[114]	International Agreement	No	Court
Equality	Equality Act 2010[115]	Law	No	Court Equality and Human Rights Commission, and National Commissions in devolved nations

[113] Health and Social Care Act 2012, UK Gov, 2012.

[114] Transforming our world: the 2030 Agenda for Sustainable Development, United Nations, 2021.

[115] Equality Act 2010, UK Gov, 2010.

< PREVIOUS SECTION NEXT SECTION >

2. A blank legal checklist to complete

This is designed to help you identify relevant laws and policies in your jurisdiction, as part of achieving Process A ('Strengthen and enforce laws that prohibit child online safety-related offences').

Policy area	Law/regulation	Status	Does it include child online safety?	Regulator/ court
Consumer rights	✎			
Child protection				
Criminal justice				
Human rights including children's rights				
Data protection				
Broadband plans				
International trade				

▶

< PREVIOUS SECTION NEXT SECTION >

2 Legal and regulatory frameworks

Policy area	Law/regulation	Status	Does it include child online safety?	Regulator/ court
Gambling				
Advertising				
Financial crimes				
Education				
Health				
International cooperation				
Equality				
Other				

< PREVIOUS SECTION NEXT SECTION >

Other resources for references:

1. Case study of Albanian oversight mechanisms[116]

The National Council for the Rights and Protection of the Child is established in law as the accountable national governance and oversight committee; and protection from online child sexual exploitation and abuse is included in key policy and legislation.

2. The Ghana Cybersecurity Act (Act 1038)[117]

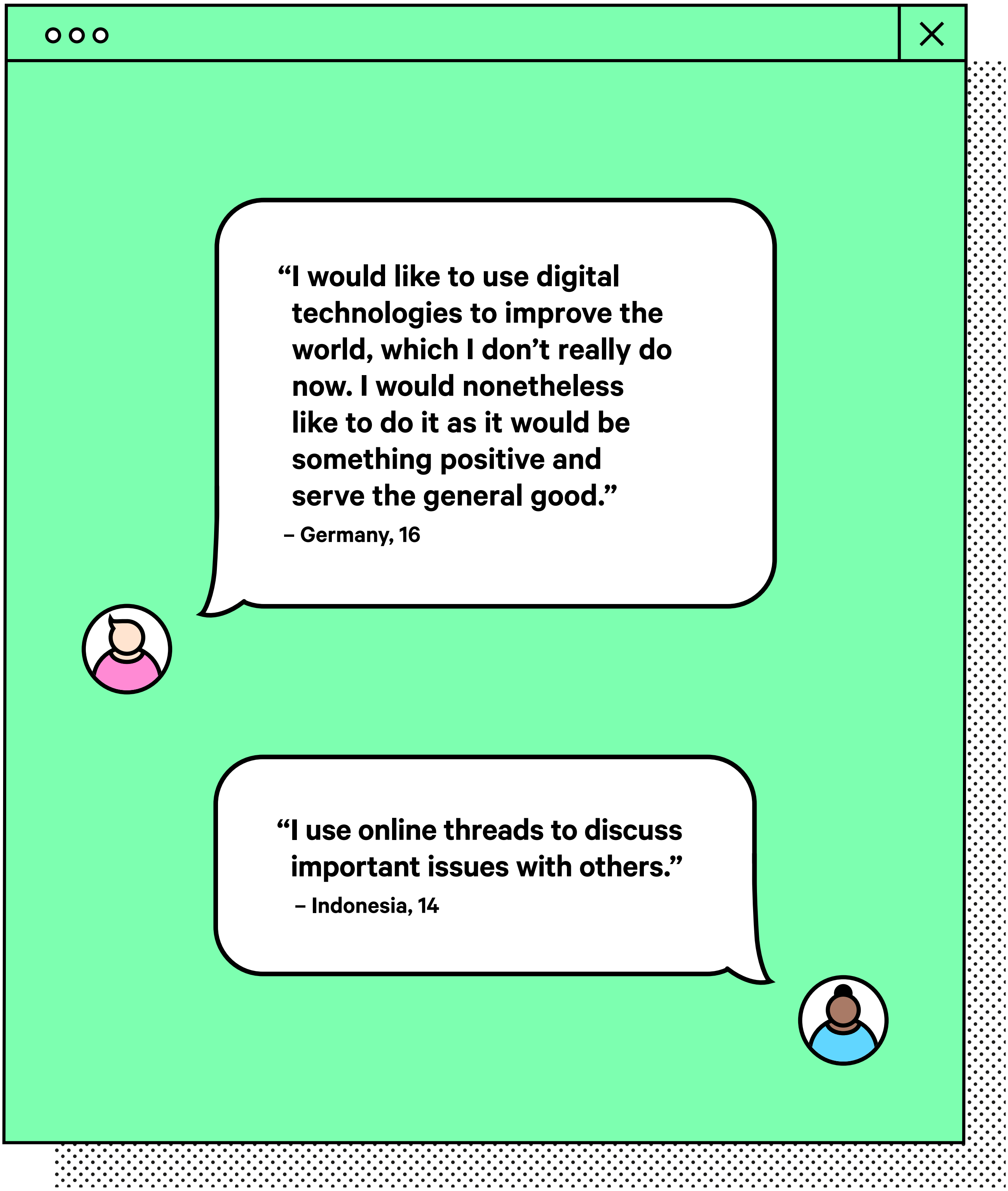
The Ghana Cybersecurity Act (Act 1038) has provisions for the protection of children online by criminalizing online sexual conducts involving children. Indecent images and photographs of children, grooming of children for sexual abuse, cyber stalking and sexual extortion are all prohibited by the law. The Act imposes some obligations on telecommunication service providers to protect children within the digital space. Further amendments have been proposed for the Children's Act (Act 560).

[116] Programming for children's protection online in Albania: A Promising Practice, UNICEF, 2020.

[117] Cybersecurity Act 2020, Government of Ghana, Ministry of Communications and Digitalisation (Act 1038), 2020.

< PREVIOUS SECTION

NEXT SECTION >



"I would like to use digital technologies to improve the world, which I don't really do now. I would nonetheless like to do it as it would be something positive and serve the general good."

– Germany, 16

"I use online threads to discuss important issues with others."

– Indonesia, 14

< PREVIOUS SECTION NEXT SECTION >

3 Personal data, identity and autonomy

> **States parties should take legislative, administrative and other measures to ensure that children's privacy is respected and protected by all organizations and in all environments that process their data. Legislation should include strong safeguards, transparency, independent oversight and access to remedy. States parties should require the integration of privacy-by-design into digital products and services that affect children. They should regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy. Where encryption is considered an appropriate means, States parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material. Such measures must be strictly limited according to the principles of legality, necessity and proportionality.**
>
> Source: General comment No. 25 (2021), para 70[118]

Objective:

To recognise the benefits of and respond to the current and emerging threats to privacy, identity and the agency of children in the digital world posed by the use of data including personal data, biometrics and automated decision making.

Model policy text:

To ensure a holistic approach to child online safety, each of the steps below is necessary.

3a. Establish or ensure existing data protection frameworks are effective in providing specific protection for children's data
Children's rights in the online environment are intimately connected with the way their data is collected, stored and used. Data protection law and regulation for children must be accessible, effective, and capable of evolving to meet emerging risks.[119] This means, not only establishing the legal and regulatory frameworks, but also making sure they work in practice and are implemented accordingly.

3b. Establish protocols for and limitations on the use of automated decision making that may affect children
Standards, laws and codes of practice should ensure that children benefit from automated systems and are not penalised through automated decision making.[120] It is particularly important to avoid the potential for discrimination through automated decision making. These protocols and limitations may apply in the context of criminal justice, social welfare, health and medicine, education, and the private sector among others. ▶

[118] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[119] General Data Protection Regulation, European Union, 2018.

[120] World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert, Office of the United Nations High Commissioner for Human Rights, 2019.

< PREVIOUS SECTION NEXT SECTION >

3c. Ensure adequate legal and regulatory protections for children's biometric data
Government and regulators should establish appropriate legal and regulatory protocols for and limitations on the use of children's biometric data in light of the principles of children's rights, purpose limitation and the requirements of child online safety policy.

3d. Establish clear guidance, laws and regulations on practices that may affect children's agency
Create legal frameworks preventing personalised targeting and tracking of children for commercial purposes based on their personal data. Establish codes on the use of recommendation systems and other automated decision-making processes or technologies that may drive children's behaviour, mould preferences and opinions, undermine reputations or limit experimentation.[121]

3e. Establish effective oversight and monitoring
Creating bodies and systems that can gather information relevant to child online safety and ensure transparency and effective implementation of children's rights and protections by business, government and other organisations.

3f. Establish frameworks to ensure transparency
Oversight should be provided by an appointed regulatory body that is sufficiently resourced and has the necessary capacity and expertise to understand the systems in use and how they impact on children's rights. The oversight body should also have access to independent researchers and experts.

[121] See for example, YouTube Data Breach Claim, McCann vs Google, 2021.

< PREVIOUS SECTION NEXT SECTION >

Roadmap to achieving the objective:

A Establish or ensure existing data protection frameworks are effective in providing specific protection for children's data

Children's rights in the online environment are intimately connected with the way their data is collected, stored and used. Data protection law and regulation for children must be accessible, effective, and capable of evolving to meet emerging risks.[122] This means, not only establishing the legal and regulatory frameworks, but also making sure they work in practice.

If yes, provide details:

If no, it will help to:

1. Look at the UK's Age Appropriate Design Code[123] which represents the gold standard of data protection for children (see 'Other Resources for Reference 2').
2. Consider the GDPR[124] as a model source for establishing broader regulation or regulation with enforcement provisions and key definitions.
3. Consider the need for specialist or separate codes, for example codes to cover data use in education and health settings, or data held by government bodies.
4. Ensure these are covered by your plan, as developed in Policy action area on Legal and regulatory framework. See Supportive tools 1 (page no. 80).

[122] General Data Protection Regulation, European Union, 2018.

[123] Age appropriate design code – Executive summary, UK Information Commissioner's Office, 2020.

[124] General Data Protection Regulation, European Union, 2018.

< PREVIOUS SECTION NEXT SECTION >

B Establish protocols for and limitations on the use of automated decision making that may affect children

Standards, laws and codes of practice should ensure that children benefit from automated systems and are not penalised through automated decision making.[125] It is particularly important to avoid the potential for discrimination through automated decision making. These protocols and limitations may apply in the context of criminal justice, social welfare, health and medicine, education, and the private sector among others.

If yes, provide details:

If no, it will help to look for recent legislation, regulation and international technical standards of AI design, audit and oversight in other jurisdictions or regional or international organisations – for example, the Artificial Intelligence Act in the EU[126] – and adapt them to your country.

[125] World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert, Office of the United Nations High Commissioner for Human Rights, 2019.

[126] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts COM/2021/206, EUR-Lex, 2021; Global Policy AI, Organisation for Economic Co-operation and Development, 2021.

< PREVIOUS SECTION NEXT SECTION >

C Ensure adequate legal and regulatory protections for children's biometric data

Government and regulators should establish appropriate legal and regulatory protocols for and limitations on the use of children's biometric data in light of the principles of children's rights, purpose limitation and the requirements of child online safety policy.

If yes, provide details:

If no, it will help to:

1. See if biometric data is covered by other national laws or regulations (e.g. data legislation). It may be that some laws that do not mention biometric data can be interpreted to include it:[127]

   A. Where it exists ensure enhanced protections for children.

   B. Where nothing is in place a provision for biometric data should be developed. It should cover biometric data for which consent has been given (for example, unlocking a phone) and where consent is not given or its use is not obvious (for example, facial recognition in school entrance systems, or fingerprint ID to get school lunch).

[127] See for example, Chile: children asked for their biometrics data to obtain food rations in schools, Privacy International, 2019.

< PREVIOUS SECTION NEXT SECTION >

D **Establish clear guidance, laws and regulations on practices that may affect children's agency**

Create legal frameworks that prevent personalised targeting and tracking of children for commercial purposes based on their personal data. Establish codes on the use of recommendation systems and other automated decision-making processes or technology that may drive children's behaviour, mould preferences and opinions, undermine reputations or limit experimentation.[128]

If yes, provide details:

If no, it will help to check for recent developments in data law, and whether regulations in other jurisdictions that ensure equitable use of personal profiling or limit excessive nudging are emerging. For example, the Age Appropriate Design Code (UK),[129] General Data Protection Regulation (GDPR, EU)[130] or Digital Services Act (EU)[131] and the Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code, UK).[132]

[128] See for example, YouTube Data Breach Claim, McCann vs Google, 2021.

[129] Age appropriate design code, UK Information Commissioner's Office, 2020.

[130] General Data Protection Regulation, European Union, 2018.

[131] The Digital Services Act: Ensuring a Safe and Accountable Online Environment, European Commission, 2019.

[132] The Code of Non-broadcast Advertising and Direct & Promotional Marketing, CAP Code, UK.

< PREVIOUS SECTION NEXT SECTION >

3 Personal data, identity and autonomy

E Establish effective oversight and monitoring

Creating bodies and systems that can gather information relevant to child online safety and ensure transparency and effective implementation of children's rights and protections by business, government and other organisations.

If yes, provide details:

If no, it will help to:

1. Ensure there is an institution or empowered body or bodies that can recommend and enforce agreed practice. For example, the National Centre for Missing & Exploited Children guidelines.[133]
2. Clarify this in the strategy developed in Policy action area on Legal and regulatory frameworks with lines of accountability and oversight (page no. 56).

[133] Our work, National Centre for Missing and Exploited Children (NCMEC).

< PREVIOUS SECTION NEXT SECTION >

F Establish frameworks to ensure transparency

Oversight should be provided by an appointed regulatory body that is sufficiently resourced and has the necessary capacity and expertise to understand the systems in use and how they impact on children's rights. The oversight body should also have access to independent researchers and experts.

If yes, provide details:

If no, it will help to ensure the chosen regulatory body is mandated by law, resourced and empowered to manage this. For example, the Information Commissioner's Office (ICO).[134] The ICO is the UK's independent authority set up to uphold information standards and rights in the public interest. Or the National Data Protection Authority (ANPD) operating under Brazil's General Data Protection Law.[135]

[134] UK Information Commissioner's Office (ICO).

[135] National Data Protection Authority (ANPD), Federal Government of Brazil.

< PREVIOUS SECTION

NEXT SECTION >

How this aligns with foundational documents:

> **The adoption of safeguards related to digital identity is critical for Governments and the United Nations as they strive to realise its full utility and potential while building trust in its use. This includes, for instance, efforts such as decentralised data storage, identification and authentication, encrypted communications and considering the incorporation of "privacy by design" principles.**
>
> Source: United Nations Secretary-General's Roadmap for Digital Cooperation, June 2020[136]

> **Where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child or, depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to processing those data. Where a child's own consent is considered insufficient and parental consent is required to process a child's personal data, States parties should require that organizations processing such data verify that consent is informed, meaningful and given by the child's parent or caregiver.**
>
> Source: General comment No. 25 (2021), para 71[137]

> **States parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations. They should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. They should also provide information to children, parents and caregivers on such matters, in child-friendly language and accessible formats.**
>
> Source: General comment No. 25 (2021), para 72[138]

[136] United Nations Secretary-General's Roadmap for Digital Cooperation, United Nations, June 2020.

[137] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[138] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

Process A ('Establish or ensure existing data protection frameworks are effective in providing specific protection for children's data') requires ensuring that all aspects of children's data are adequately protected in legislation and regulation. This tool is designed to support policy makers to think about the breadth of issues data protection frameworks need to address for children.

Supportive tools:

1. Checklist to ensure comprehensive data protection legislation for children

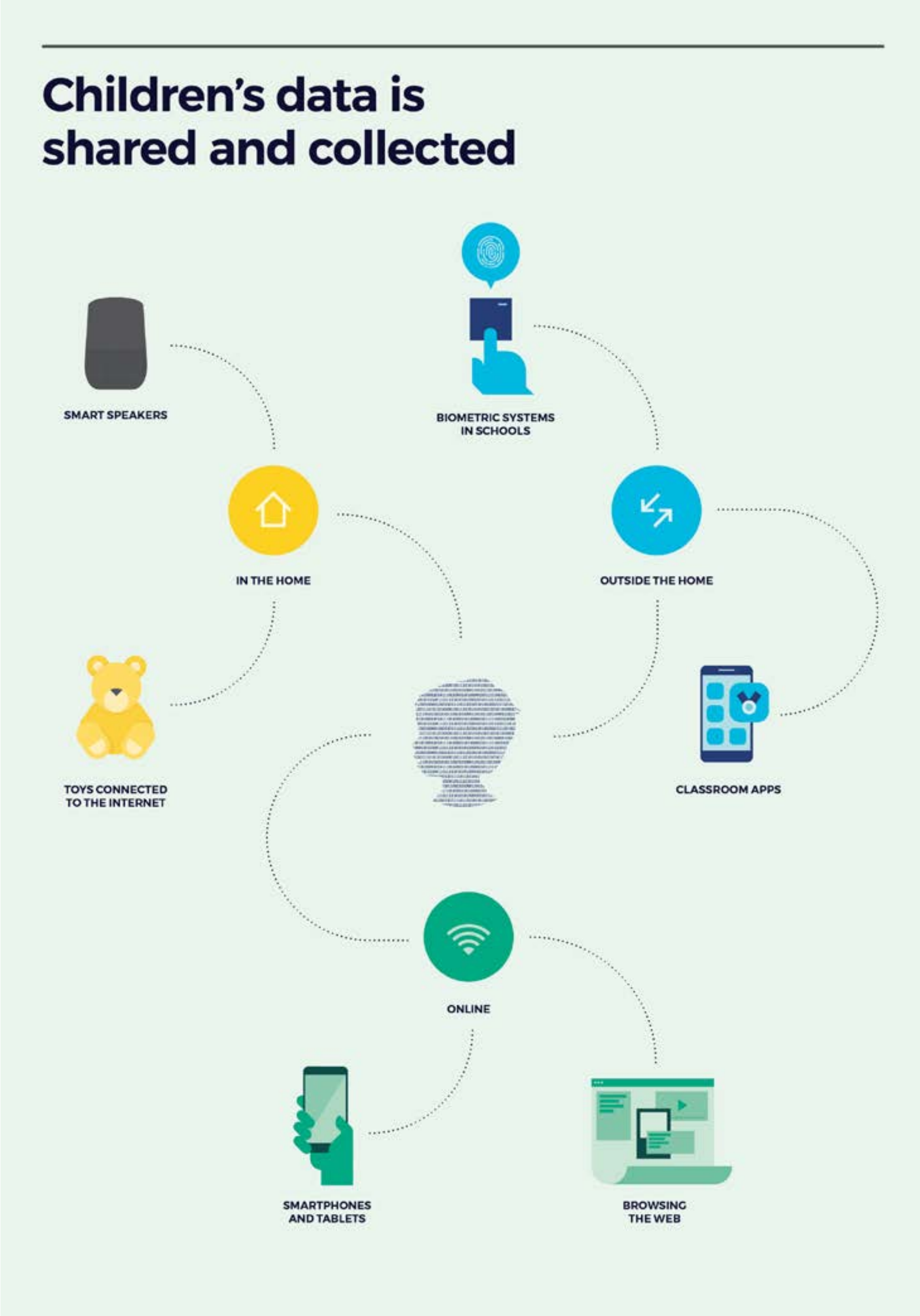
Do you have data protection frameworks that cover:	✎
Collection	
Storage	
Use	
Education data	
Health data	
Government and administrative data	
Data used for automated decision making	
Data used in other AI systems	
Biometric data	

< PREVIOUS SECTION

NEXT SECTION >

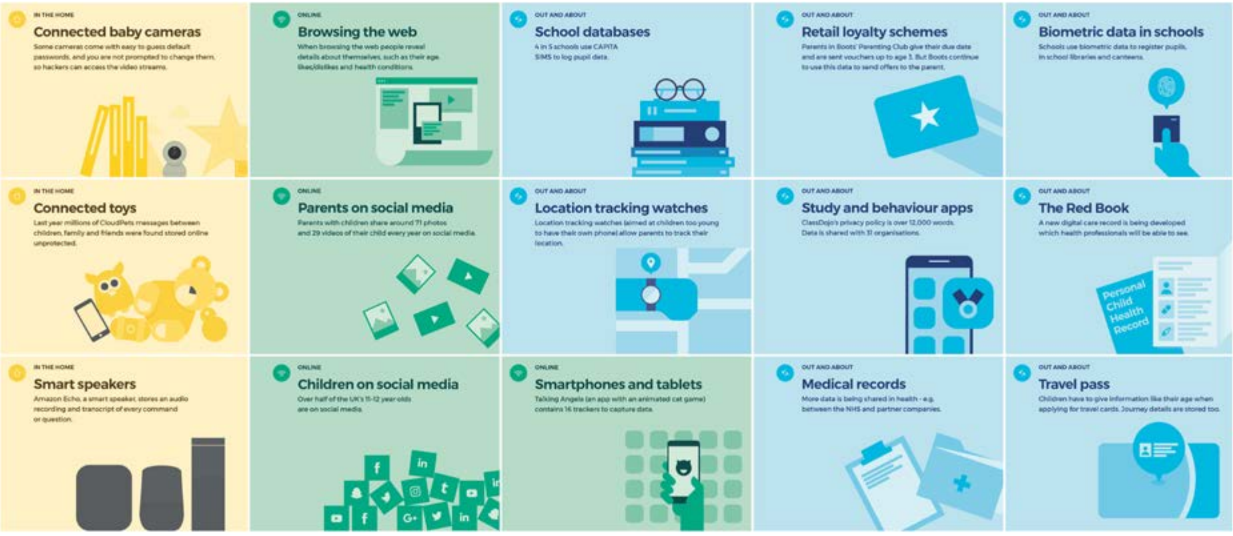
Other resources for reference:

1. **Visuals to help understand the breadth and volume of children's data collected**



Source: Children's Commissioner 'Who knows what about me' Infographic[139]

[139] Who knows what about me?, Children's Commissioner, 2018.


IN THE HOME
Connected baby cameras
Some cameras come with easy to guess default passwords, and you are not prompted to change them, so hackers can access the video streams.
ONLINE
Browsing the web
When browsing the web people reveal details about themselves, such as their age, likes/dislikes and health conditions.
OUT AND ABOUT
School databases
4 in 5 schools use CAPITA SIMS to log pupil data.
OUT AND ABOUT
Retail loyalty schemes
Parents in Boots' Parenting Club give their due date and are sent vouchers up to age 3. But Boots continue to use this data to send offers to the parent.
OUT AND ABOUT
Biometric data in schools
Schools use biometric data to register pupils, in school libraries and canteens.
IN THE HOME
Connected toys
Last year millions of CloudPets messages between children, family and friends were found stored online unprotected.
ONLINE
Parents on social media
Parents with children share around 71 photos and 29 videos of their child every year on social media.
OUT AND ABOUT
Location tracking watches
Location tracking watches (aimed at children too young to have their own phone) allow parents to track their location.
OUT AND ABOUT
Study and behaviour apps
ClassDojo's privacy policy is over 12,000 words. Data is shared with 11 organisations.
OUT AND ABOUT
The Red Book
A new digital care record is being developed which health professionals will be able to see.
Personal Child Health Record
IN THE HOME
Smart speakers
Amazon Echo, a smart speaker, stores an audio recording and transcript of every command or question.
ONLINE
Children on social media
Over half of the UK's 11-12 year olds are on social media.
ONLINE
Smartphones and tablets
Talking Angela (an app with an animated cat game) contains 16 trackers to capture data.
OUT AND ABOUT
Medical records
More data is being shared in health - e.g. between the NHS and partner companies.
OUT AND ABOUT
Travel pass
Children have to give information like their age when applying for travel cards. Journey details are stored too.

Source: Children's Commissioner 'Who knows what about me' Infographic[140]

2. Case Study of the UK's Age Appropriate Design Code[141]

The UK has implemented a ground breaking piece of legislation that addresses how children's data can be used, called the *Age Appropriate Design Code*.

> **"This code addresses how to design data protection safeguards into online services to ensure they are appropriate for use by, and meet the development needs of, children. It reflects the increasing concern about the position of children in society and the modern digital world in particular. There is agreement at international level and within the UK that much more needs to be done to create a safe online space for them to learn, explore and play. This code achieves this not by seeking to protect children from the digital world, but by protecting them within it."**

The code sets out 15 standards of age appropriate design reflecting a risk-based approach. The focus is on providing default settings which ensures that children have the best possible access to online services whilst minimising data collection and use, by default. The principles are:

1. Best Interests of the Child
2. Data Protection Impact Assessments
3. Age-Appropriate Application
4. Transparency
5. Detrimental Use of Data
6. Policies and Community Standards
7. Default Settings
8. Data Minimisation
9. Data Sharing
10. Geolocation
11. Parental Controls
12. Profiling
13. Nudge Techniques
14. Connected Toys and Devices
15. Online Tools

[140] Who knows what about me?, Children's Commissioner, 2018.

< PREVIOUS SECTION NEXT SECTION >

The Age Appropriate Design Code came into force in the UK on 2nd September 2021. It has its foundations in the EU-wide General Data Protection Regulation (GDPR) and is therefore likely to be familiar in countries with GDPR compliant regimes. It is widely considered to be the most advanced data protection regime for children in the world. Since its implementation, services have announced a raft of changes to their engagement with children, including the following:

- On Instagram, adults cannot direct message under 18s who do not follow them.
- Google's SafeSearch will be turned on by default for all under 18s.
- On YouTube, autoplay is turned off for under 18s and break and bedtime reminders are turned on by default.
- Children under the age of 16 are not able to host livestreams on TikTok and have push notifications switched off after 9pm.
- Google and Facebook will stop behavioural advertising to children.

Specific sectors or types of information may be subject to additional provisions, for example, health data, financial data and education data. These may be other areas that need additional codes or add-ons but all must meet a high bar of privacy and be in the best interests of children.

3. UNICEF's Manifesto for the Better Governance of Children's Data[142]

UNICEF's working group on data governance has produced a report documenting the reasons for, and principles of better data governance of children's data. The ten action points of the manifesto focus on using data in the best interests of children, working with children themselves to understand beneficial uses, and filling the knowledge gap between technology and the institutions and people that use it.

4. OECD Privacy Framework[143]

The OECD Privacy Framework brings together the key components of the OECD privacy framework, based on their revised Privacy Guidelines:

BASIC PRINCIPLES OF NATIONAL APPLICATION:

Collection Limitation Principle
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

[141] Age Appropriate Design Code, UK Information Commissioner's Office, 2020.

[142] The Case for Better Governance of Children's Data: A Manifesto, UNICEF's Office of Global Insight and Policy, 2021.

[143] Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development, 2013.

< PREVIOUS SECTION NEXT SECTION >

Purpose Specification Principle
The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle
Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle
There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle
Individuals should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

b) to have communicated to them, data relating to them

   i. within a reasonable time;

   ii. at a charge, if any, that is not excessive;

   iii. in a reasonable manner; and

   iv. in a form that is readily intelligible to them;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to them and, if the challenge is successful. to have the data erased, rectified, completed or amended.

Accountability Principle
A data controller should be accountable for complying with measures which give effect to the principles stated above.

< PREVIOUS SECTION NEXT SECTION >

Basic principles of international application: Free flow and legitimate restrictions

- A data controller remains accountable for personal data under its control without regard to the location of the data.

- A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

- Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

5. **European Union General Data Protection Regulation (text and tools)**[144]
The General Data Protection Regulation (GDPR) is a privacy and security law authorised by the European Union. It requires businesses operating inside and outside European countries to lawfully use EU citizens' personal data.

6. **The European Digital Strategy (including proposals on Artificial Intelligence and Data)**[145]
This is the guide to understand how the European Union shapes their digital future. The European Digital Strategy aims to develop a single market for all companies to compete in equal terms without violating consumers' privacy rights and to shape a better digital society in the region and globally.

7. **Irish Data Protection Commissioner Fundamentals for a Child Oriented Approach to Data Processing (The Fundamentals)**[146]
Drawn up by the Irish Data Protection Commission (DPC), The Fundamentals aim to improve standards of data processing. They serve as guidance for organisations involved in processing children's data, with the principles generated under GDPR.

8. **UNICEF Memo on Artificial Intelligence and Children's Rights**[147]
The Memo provided by UNICEF outlines key elements on how AI influences children's rights in different areas such as popular video-watching platform YouTube, smart toys and AI in education. It also puts forward initial recommendations to policy makers, corporations, parents and educators.

9. **EU Fundamental Rights Agency Report – Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights**[148]
The information technology (IT) systems established by the EU plays a vital role in the regional security such as migration management and combating terrorism and serious crime. However, the systems' impacts on fundamental rights have yet to be explored. For example, with the framework provided by OHCHR Convention on the Rights of the Child in Article 24, the report in chapter 7 strengthens that the systems should put the child's best interests first when collecting biometric identifiers.

[144] General Data Protection Regulation, European Union, 2018.
[145] Shaping Europe's digital future, European Union, 2020.
[146] Fundamentals for a Child-Oriented Approach to Data Processing, Ireland Data Protection Commission, 2020.
[147] Artificial Intelligence and Children's Rights, United Nations Children's Fund, 2019.
[148] Under watchful eyes: biometrics, EU IT systems and fundamental rights, European Union Agency for Fundamental Rights, 2018.

10. **UNICEF's Guidance on AI and Children**[149]
While AI systems have been widely deployed by countries, concerns about this new technology have also driven governments, businesses and civil society to develop principles to leverage them via ethics. Although human rights have been included in these AI strategies, children's rights in particular have not yet been sufficiently addressed. In this guidance, UNICEF aims to raise awareness of children's rights and provide recommendations to different parties – mainly policy makers and business leaders – on child-related AI

AI-powered voice assistants and chatbots

Virtual voice assistants and chatbots utilise NLP (Natural Language Processing), automatic speech recognition and machine learning to recognise verbal commands, identify patterns retrieve information and generate responses. While these systems have not always been built or tailored for children, millions of children are being shaped by them either emotionally or behaviourally. Proponents of these technologies have cited benefits that include support for children with visual impairments or limited mobility, and new ways of learning and stoking children's curiosity and creativity. Additionally, some chatbots aim to make studying easier and more time-efficient for students.

However, the use of chatbots can lead to additional risks for children, especially in mental health, when bots do not recognise appeals for help or provide inadequate advice. For instance, a 2018 testing of two mental health chatbots by the BBC revealed that the applications failed to properly handle children's reports of sexual abuse, even though both apps had been considered suitable for children. According to a UNICEF briefing, "when not designed carefully, chatbots can compound rather than dispel distress" which is "particularly risky in the case of young users who may not have the emotional resilience to cope with a negative or confusing chatbot response experience". Moreover, chatbots may pose several security threats including spoofing (impersonating someone else), tampering with data, data theft and vulnerability to cyber attacks, and may enforce bias, given that they often select a predetermined reply based on the most matching keywords or similar wording pattern.

Further concerns related to chatbot and personal assistant technologies relate to privacy and data ownership. For instance, given that voice assistants typically rely on storing voice recordings to facilitate the system's continuous learning, child rights' advocates have raised questions over the lack of clarity in company data retention policies and child and parental consent.

Facial recognition for biometric identification

Facial recognition systems employ computer vision techniques and machine learning algorithms to determine, process and analyse a person's facial features with a wide range of aims, such as verifying an individual's identity against an existing record. For identification purposes, it may be used in border management, crime analysis and prevention, and school surveillance for claimed

[149] Policy guidance on AI for children, United Nations Children's Fund, 2020.

< PREVIOUS SECTION NEXT SECTION >

> **reasons of improved security. Facial recognition is increasingly being used as a means of a digital identity "credential" for both legal and functional identification. While not a replacement for legal ID, which makes people visible to a State and is a recognised right, this technology may more quickly or easily validate an existing identity record.**
>
> **The associated human and child rights risks and limitations are great. Privacy advocates have warned against its true use in government mass surveillance efforts as a law enforcement investigative tool, particularly as it can be utilised to profile, track and suppress vulnerable communities. In some cases, these systems also raise issues of meaningful consent as people may not know who is collecting the biometric data or even that it is being collected, how it is being stored or how it could be applied. Furthermore, inaccuracies in facial recognition detection continue to persist, including less reliable matching for children's faces and other groups based on gender and ethnicity, such as women of colour. As a consequence, this could cement existing social biases and lead to discrimination or further marginalisation of minority communities.**
>
> Source: Policy guidance on AI for children, United Nations Children's Fund, 2020[150]

1. **Children's Code: Additional Resources**[151]
   This website hosts all of the UK's Information Commissioner's Office's additional resources about the Age Appropriate Design Code, including Frequently Asked Questions and a Data Protection Impact Assessment Template.

2. **5Rights Foundation's Demystifying the Age Appropriate Design Code**[152]
   This is a booklet for children about the development of the UK's Age Appropriate Design Code.

[150] Policy guidance on AI for children, United Nations Children's Fund, 2020,

[151] Children's code: additional resources, ICO 2021.

[152] Demystifying the Age Appropriate Design Code, 5Rights Foundation, 2020.

< PREVIOUS SECTION

NEXT SECTION >

“When expressing yourself online, you have to keep in mind not to give away any personal information...”
– Canada, 10

“I don’t think you should have restrictions about how you could express yourself because everyone should be able to talk about how they feel about something.”
– Canada, 12

< PREVIOUS SECTION NEXT SECTION >

4 Response and support systems

> **States parties should provide children with child-sensitive and age-appropriate information in child-friendly language on their rights and on the reporting and complaint mechanisms, services and remedies available to them in cases where their rights in relation to the digital environment are violated or abused. Such information should also be provided to parents, caregivers and professionals working with and for children.**
>
> Source: General comment No. 25 (2021), para 49[153]

> **Capability 4 Model National Response – Law Enforcement Good Practice**
>
> **For countries that do not currently have a dedicated CSEA law enforcement capability in place, the national law enforcement agency should identify and commit to building this capability.**
>
> **For countries that already have a dedicated CSEA law enforcement capability but still need to develop a multi-stakeholder approach, the inclusion of dedicated child protection professionals to work alongside investigators is a significant first step. Leading practice child protection principles for law enforcement should be followed at all times when planning and conducting a CSEA investigation; this will ensure the needs and rights of the child are always paramount. The multi-stakeholder approach will provide an enhanced level of protection and support for the victim and help achieve best evidence from the victim – increasing the likelihood of a successful prosecution. Sharing best practice across the region is also desirable.**
>
> Source: WeProtect Global Alliance Model National Response[154]

Objective:

To establish a coordinated multi-stakeholder framework to tackle risks for children online, in particular child exploitation and abuse (CSEA): including effective legal and regulatory enforcement mechanisms, prevention, remedies and access to expert advice on child online safety.

[153] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[154] Child sexual exploitation and abuse (CSEA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline.

< PREVIOUS SECTION NEXT SECTION >

Model policy text:

To ensure a holistic approach to child online safety, each of the steps below is necessary.

4a. Notice and takedown

Government institutions will work with experts, the enforcement community and industry to establish and monitor effective protocols for the notice and takedown of illegal and harmful material. Among other things, this will require the development of protocols to ensure, and legislation to permit, local internet service providers (ISPs) to restrict access to hosts that fail to take down notified content or persistently breach laws or other regulatory requirements on child online safety.

4b. Establish processes for offender risk management in relation to CSEA

An effective multi-stakeholder offender management process should be established, drawing upon international standards of good practice. Law enforcement and other criminal justice practitioners will be trained to recognise and investigate offending behaviours. Offender risk management is an essential component of child online safety, as individuals or groups of offenders can reach large numbers of child victims online.

4c. Provide adequate resources for psycho-social support for primary and secondary child victims and their families

Organisations training practitioners in the mental health, psychology and social work fields who work with vulnerable children must be required to have a basic understanding of child online safety issues.[155] Child online safety should be integrated into broader child safety and protection systems, such as safeguarding in schools or violence against children (VAC).

4d. Establish victim detection and protection frameworks

A key aim in the prevention of online harm will be to consider the needs of vulnerable children and how best to support them. One Stop Centres act as an initial umbrella institution for victims of abuse: these provide access to a range of essential services, from medical to legal support, in one centralised location. They offer a framework for safeguarding and child protection procedures, provide support for victims, and rapidly escalate reports of online crimes to the relevant authorities.[156]

4e. Ensure relevant frameworks do not criminalise children

It is important to establish appropriate frameworks for managing children who may find themselves in conflict with the law in the context of child online safety – for example, in cases of cyberbullying, spreading malicious information or hacking. Where possible, children should be diverted from the criminal justice system, and opportunities for counselling or restorative justice should be preferred. Particular care should be taken to ensure that a child's circumstances are fully understood. For example, a child's behaviour might be the product of bullying, grooming or some other form of coercion.

[155] What Works to Prevent Violence Against Women and Girls Evidence Reviews Paper 3: Response mechanisms to prevent violence, What Works, 2015. p.28.

[156] Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, WeProtect Global Alliance, 2016.

< PREVIOUS SECTION NEXT SECTION >

Roadmap to achieving the objective:

A Notice and takedown

Government institutions should work with experts, the enforcement community and industry to establish and monitor effective protocols for the notice and takedown of illegal and harmful material. Among other things, this will require the development of protocols to ensure, and legislation to permit, local internet service providers (ISPs) to restrict access to hosts that fail to take down notified content or persistently breach laws or other regulatory requirements on child online safety.

If yes, provide details:

If no, it will help to:

1. Develop and implement plans to address the gaps in provision. See Supportive tools 1 (page no. 97).
2. Consider the foundational documents provided in Key Documents and other resources, particularly the MNR,[157] for guidance (see Other Resources for Reference 1).

[157] Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, WeProtect Global Alliance, 2016.

< PREVIOUS SECTION NEXT SECTION >

B Establish processes for offender risk management in relation to CSEA

An effective multi-stakeholder offender management process should be established, drawing upon international standards of good practice. Law enforcement and other criminal justice practitioners will be trained to recognise and investigate offending behaviours. Offender risk management is an essential component of child online safety, as individuals or groups of offenders can reach large numbers of child victims online.

If yes, provide details:

If no, it will help to:

1. Gather existing expertise to create a rich knowledge base, for example the National Crime Agency[158] and Europol.[159]
2. If necessary, reach out to international or regional experts for support, such as the National Center for Missing & Exploited Children,[160] Internet Watch Foundation,[161] INTERPOL[162] and ECPAT.[163]

[158] About us, National Crime Agency.

[159] About Europol, Europol.

[160] Our work, National Center for Missing and Exploited Children.

[161] About Us, Internet Watch Foundation (IWF).

[162] Who we are, INTERPOL.

[163] Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International, 2016.

< PREVIOUS SECTION NEXT SECTION >

C Provide adequate resources for psycho-social support for primary and secondary child victims and their families

Organisations training practitioners in the mental health, psychology and social work fields who work with vulnerable children must be required to have a basic understanding of child online safety issues.[164] Child online safety should be integrated into broader child safety and protection systems.

If yes, provide details:

If no, it will help to:

1. Establish some long-term capacity building in the area of child sexual exploitation and abuse, as part of your ongoing plan. See Supportive tools 1 in the Policy action area on Training for support in identifying necessary training needs to grow capacity (page no. 119).

2. If necessary, reach out to international or regional experts for support, such as the National Center for Missing & Exploited Children[165] Internet Watch Foundation,[166] INTERPOL[167] and ECPAT.[168]

[164] Child sexual abuse (CSA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline.

[165] Our work, National Center for Missing and Exploited Children.

[166] About Us, Internet Watch Foundation (IWF).

[167] Who we are, INTERPOL.

[168] Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International, 2016.

< PREVIOUS SECTION NEXT SECTION >

D Establish victim detection and protection frameworks

A key aim in the prevention of online harm will be to consider the needs of vulnerable children and how best to support them. The capabilities of One Stop Centres will be strengthened to ensure they follow safeguarding and child protection procedures, provide support for victims, and rapidly escalate reports of online crimes to the relevant authorities.

If yes, provide details:

If no, it will help to:

1. Study existing One Stop Centres (such as the MNR[169] provided in Other resources for reference 1). For example, Police Scotland.[170]
2. If necessary, seek international or regional expertise to bring together the network of necessary skills, such as the National Center for Missing & Exploited Children,[171] Internet Watch Foundation,[172] INTERPOL[173] and ECPAT.[174]

[169] Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, WeProtect, 2016.

[170] Internet Safety, Police Scotland.

[171] Our work, National Centre for Missing and Exploited Children (NCMEC).

[172] About Us, Internet Watch Foundation (IWF).

[173] Who we are, INTERPOL.

[174] Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International, 2016.

< PREVIOUS SECTION NEXT SECTION >

E Ensure relevant frameworks do not criminalise children

It is important to establish appropriate frameworks for managing children who may find themselves in conflict with the law in the context of child online safety – for example, in cases of cyberbullying, spreading malicious information or hacking. Where possible, children should be diverted from the criminal justice system and opportunities for counselling or restorative justice should be preferred. Particular care should be taken to ensure that a child's circumstances are fully understood. A child's behaviour might be the product of bullying, grooming or some other form of coercion.

If yes, provide details:

If no, it will help to:

1. Involve your justice ministry in articulating existing law(s).
2. Consult key stakeholders, including children, young people and parents/carers to amend or update laws and regulatory guidance where necessary.
3. Seek child's rights expertise to ensure that the rehabilitation and protection of minors, rather than punishment (except in the most serious cases), can be achieved.

How this aligns with foundational documents:

> **For countries that do not currently have a dedicated CSEA law enforcement capability in place, the national law enforcement agency should identify and commit to building this capability: this includes the identification of dedicated officers who will remain in post for a minimum period (suggested minimum of two years); the allocation of an appropriate venue to accommodate such resources; the acquisition of essential equipment; the provision of specialist CSEA training and techniques; psychological health and wellness support for officers; and the development and delivery of CSEA awareness-raising training for local law enforcement across the country. For countries that already have a dedicated CSEA law enforcement capability but still need to develop a multi-stakeholder approach, the inclusion of dedicated child protection professionals to work alongside investigators is a significant first step. Leading practice child protection principles for law enforcement should be followed at all times when planning and conducting a CSEA investigation; this will ensure the needs and rights of the child are always paramount. The multi-stakeholder approach will provide an enhanced level of protection and support for the victim and help achieve best evidence from the victim – increasing the likelihood of a successful prosecution. Sharing best practice across the region is also desirable.**
>
> Source: WeProtect Global Alliance Model National Response[175]

[175] Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, WeProtect Global Alliance, 2016.

< PREVIOUS SECTION NEXT SECTION >

Supportive tools:

1. Checklist to develop adequate notice and takedown procedures

Process A (‘Notice and takedown’) starts by identifying the gaps in notification and takedown systems. This checklist is designed to support policy makers to identify the steps and requirements needed to ensure illegal and harmful content can be swiftly removed once it is identified.

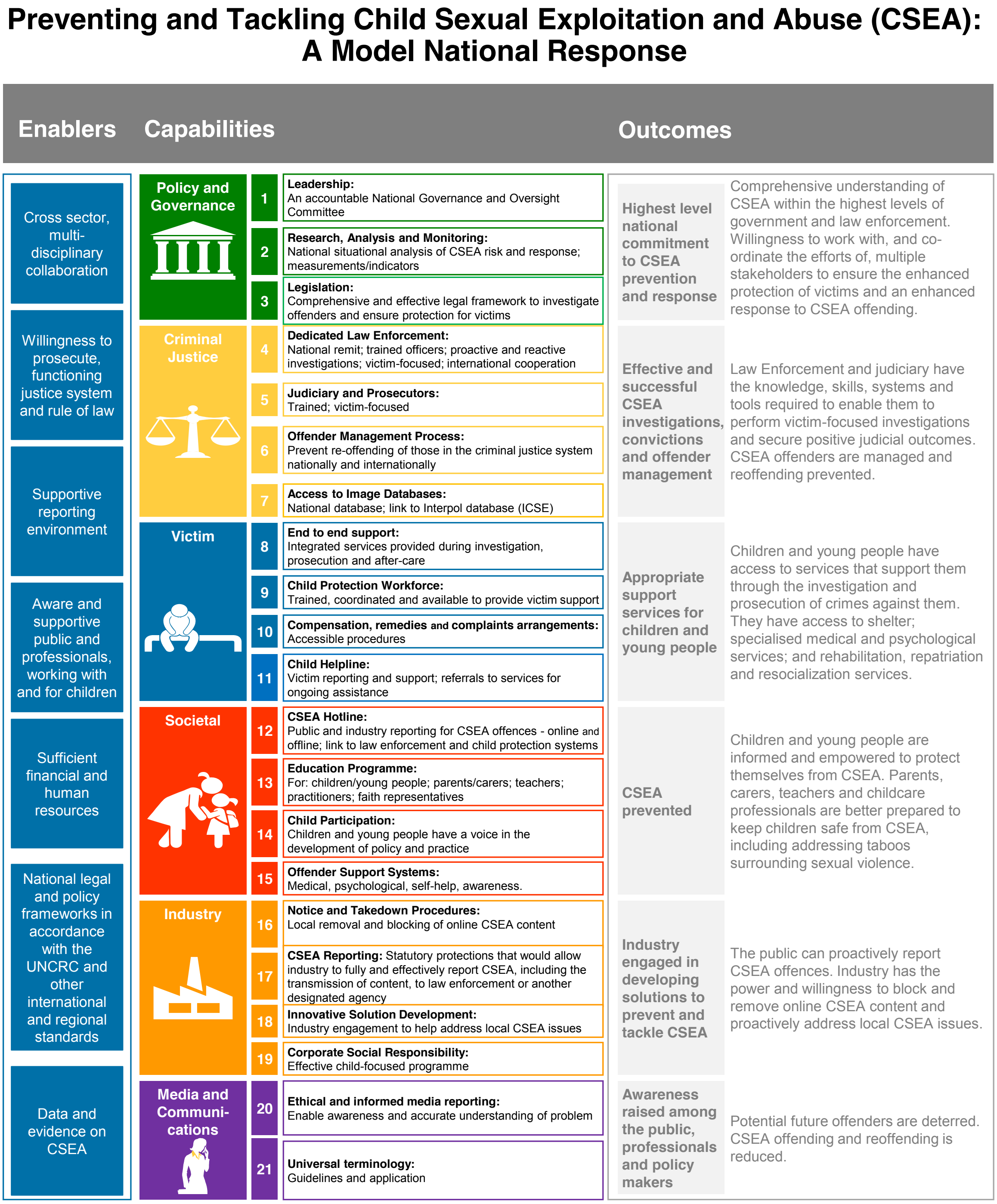
	Legal definition of illegal content articulated	Legal requirements to remove illegal content articulated	Timely process to remove illegal content required (‘takedown notices’)	Legal definition of harmful but not illegal content articulated	Legal requirements to remove harmful content articulated	Timely process to remove harmful content required (‘takedown notices’)
Internet service providers	✎					
Social media platforms						
Streaming platforms						
Cloud and other hosting services						
Other						

< PREVIOUS SECTION

NEXT SECTION >

Other resources for reference:

1. WeProtect Global Alliance's Model National Response (MNR) working examples[176]



Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response

Enablers

- Cross sector, multi-disciplinary collaboration
- Willingness to prosecute, functioning justice system and rule of law
- Supportive reporting environment
- Aware and supportive public and professionals, working with and for children
- Sufficient financial and human resources
- National legal and policy frameworks in accordance with the UNCRC and other international and regional standards
- Data and evidence on CSEA

Capabilities			Outcomes	
Policy and Governance	1	**Leadership:** An accountable National Governance and Oversight Committee	Highest level national commitment to CSEA prevention and response	Comprehensive understanding of CSEA within the highest levels of government and law enforcement. Willingness to work with, and co-ordinate the efforts of, multiple stakeholders to ensure the enhanced protection of victims and an enhanced response to CSEA offending.
	2	**Research, Analysis and Monitoring:** National situational analysis of CSEA risk and response; measurements/indicators		
	3	**Legislation:** Comprehensive and effective legal framework to investigate offenders and ensure protection for victims		
Criminal Justice	4	**Dedicated Law Enforcement:** National remit; trained officers; proactive and reactive investigations; victim-focused; international cooperation	Effective and successful CSEA investigations, convictions and offender management	Law Enforcement and judiciary have the knowledge, skills, systems and tools required to enable them to perform victim-focused investigations and secure positive judicial outcomes. CSEA offenders are managed and reoffending prevented.
	5	**Judiciary and Prosecutors:** Trained; victim-focused		
	6	**Offender Management Process:** Prevent re-offending of those in the criminal justice system nationally and internationally		
	7	**Access to Image Databases:** National database; link to Interpol database (ICSE)		
Victim	8	**End to end support:** Integrated services provided during investigation, prosecution and after-care	Appropriate support services for children and young people	Children and young people have access to services that support them through the investigation and prosecution of crimes against them. They have access to shelter; specialised medical and psychological services; and rehabilitation, repatriation and resocialization services.
	9	**Child Protection Workforce:** Trained, coordinated and available to provide victim support		
	10	**Compensation, remedies and complaints arrangements:** Accessible procedures		
	11	**Child Helpline:** Victim reporting and support; referrals to services for ongoing assistance		
Societal	12	**CSEA Hotline:** Public and industry reporting for CSEA offences - online and offline; link to law enforcement and child protection systems	CSEA prevented	Children and young people are informed and empowered to protect themselves from CSEA. Parents, carers, teachers and childcare professionals are better prepared to keep children safe from CSEA, including addressing taboos surrounding sexual violence.
	13	**Education Programme:** For: children/young people; parents/carers; teachers; practitioners; faith representatives		
	14	**Child Participation:** Children and young people have a voice in the development of policy and practice		
	15	**Offender Support Systems:** Medical, psychological, self-help, awareness.		
Industry	16	**Notice and Takedown Procedures:** Local removal and blocking of online CSEA content	Industry engaged in developing solutions to prevent and tackle CSEA	The public can proactively report CSEA offences. Industry has the power and willingness to block and remove online CSEA content and proactively address local CSEA issues.
	17	**CSEA Reporting:** Statutory protections that would allow industry to fully and effectively report CSEA, including the transmission of content, to law enforcement or another designated agency		
	18	**Innovative Solution Development:** Industry engagement to help address local CSEA issues		
	19	**Corporate Social Responsibility:** Effective child-focused programme		
Media and Communi-cations	20	**Ethical and informed media reporting:** Enable awareness and accurate understanding of problem	Awareness raised among the public, professionals and policy makers	Potential future offenders are deterred. CSEA offending and reoffending is reduced.
	21	**Universal terminology:** Guidelines and application		

[176] Working Examples of Model National Response Capabilities and Implementation, WeProtect, 2018.

< PREVIOUS SECTION

NEXT SECTION >

2. Australia's Bill for an Online Safety Act[177]

Australia's Online Safety Act includes:

- □ Updates on previous Australian legislation that is working well (specifically, the *Enhancing Online Safety Act 2015* and its image-based abuse scheme).
- □ A set of core basic online safety expectations for social media services, relevant electronic services and designated internet services, clearly stating community expectations and outlining mandatory reporting requirements.
- □ An enhanced cyberbullying scheme for Australian children to capture a range of online services, not just social media platforms.
- □ A new cyber abuse scheme for Australian adults, to facilitate the removal of serious online abuse and harassment.
- □ A modernised online content scheme, to replace the schemes in Schedules 5 and 7 of the Broadcasting Services Act 1992 (BSA). The Bill will create new classes of harmful online content and will reinvigorate out-of-date industry codes to address such content.
- □ New abhorrent/violent material blocking arrangements that allow the eSafety Commissioner to respond rapidly to an online crisis event, such as the Christchurch terrorist attacks, by requesting that internet service providers block access to sites hosting seriously harmful content.
- □ Consistent takedown requirements for image-based abuse, cyber abuse, cyberbullying and harmful online content, requiring internet service providers to remove such material within 24 hours of receiving a notice from the eSafety Commissioner.

3. Tools from EndOCSEA@Europe[178]

EndOCSEA was conceived to ensure that the rights of children are protected through effective multi-national, interdisciplinary and cross-sectoral cooperation and child-friendly measures to prevent and combat child sexual exploitation and abuse facilitated by ICTs (OCSEA) at pan-European level.

The project includes three mutually reinforcing components, each aimed at:

- □ setting up enabling environments for cross-sector, multidisciplinary collaboration at national and regional levels, by strengthening national governance structures and conducting situation analysis of OCSEA risks and responses in national and pan-European contexts;
- □ supporting legislative and procedural reforms, training and improved capacities of law enforcement officials, the judiciary and prosecutors, and promoting multidisciplinary interagency cooperation for end-to-end support for victims; and
- □ addressing societal capabilities with an emphasis on awareness raising, education of key target groups and the empowerment of children.

[177] Consultation on a Bill for a new Online Safety Act, Department of Infrastructure, Transport, Regional Development and Communications, 2020.

[178] End Online Child Sexual Exploitation and Abuse, Council of Europe, 2020.

< PREVIOUS SECTION

NEXT SECTION >

4. **Council of Europe Convention on Cybercrime (Budapest Convention)**[179]
This is an EU treaty on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child sexual abuse material and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

5. **INHOPE Hotline guidelines**[180]
The mission of INHOPE is to support the network of hotlines combating online child sexual abuse material (CSAM). INHOPE is made up of multiple hotlines around the world, that operate in all EU member states, Russia, South Africa, North and South America, Asia, Australia and New Zealand. INHOPE supports the hotlines and their partner organisations through training, best practices, quality assurance and staff welfare.

6. **UNICEF and GSMA Resources about Notice and Take Down**[181]
This is guidance for internet service providers about notice and takedown policies and procedures, to prevent the misuse of their services for sharing child sexual abuse material.

7. **R;pple Suicide Prevention**[182]
R;pple Suicide Prevention is an online monitoring tool designed to present a visual page on a user's device as soon as they are flagged as searching for a harmful keyword or phrase as listed within the R;pple monitoring tool configuration. Keywords and phrases include any words or terminology which have been identified as linking to potentially damaging online content.

8. **Case Study of Albania's approach to supporting survivors**[183]
The concept of end-to-end support is well established in this case study. There is an immediate process of psycho-social counselling that is set in motion for children who report online violence to the Albanian National Child Helpline, ALO 116 111, and there is a procedure for referral to the appropriate authorities, such that in 2019, all of the children reporting who required it were referred. Extensive investment in capacity building of the social welfare workforce has seen a revised curriculum for social work introduced, with online child violence reporting and response assimilated into the Albanian School of Public Administration standing programme for in-service training.

9. **The Cambodia National Action Plan to Prevent and Respond to Online Child Sexual Exploitation 2021-2025**[184]
The plan was developed by the Technical Working Group on Online Child Sexual Exploitation, comprising 11 government ministries, UNICEF and various NGOs. Recognising the nexus between child sexual exploitation and abuse online and offline, this action plan sits within the broader framework of the Action Plan to Prevent and Respond to Violence against Children 2017-2021, as well as the next round starting in 2022.

[179] Budapest Convention, Council of Europe, 2021.

[180] Our Story, INHOPE, 2021.

[181] Company policies and practices to remove online child sexual abuse material, United Nations Children's Fund and GSMA, 2016.

[182] R;pple Suicide Prevention, R;pple, 2021.

[183] Programming for children's protection online in Albania: A Promising Practice, United Nations Children's Fund, 2020.

[184] Official Launch of the National Action Plan to Prevent and Respond to Online Child Sexual Exploitation in Cambodia 2021-2025.

< PREVIOUS SECTION NEXT SECTION >

10. **Internet Watch Foundation (IWF)**[185]
IWF search for, stop, remove and prevent child sexual abuse imagery online. They use their unique, trusted data to research new trends, tactics and methods being employed by online perpetrators. They channel this expertise to develop cutting edge services, to help the tech community prevent, disrupt and remove online child sexual abuse imagery globally.

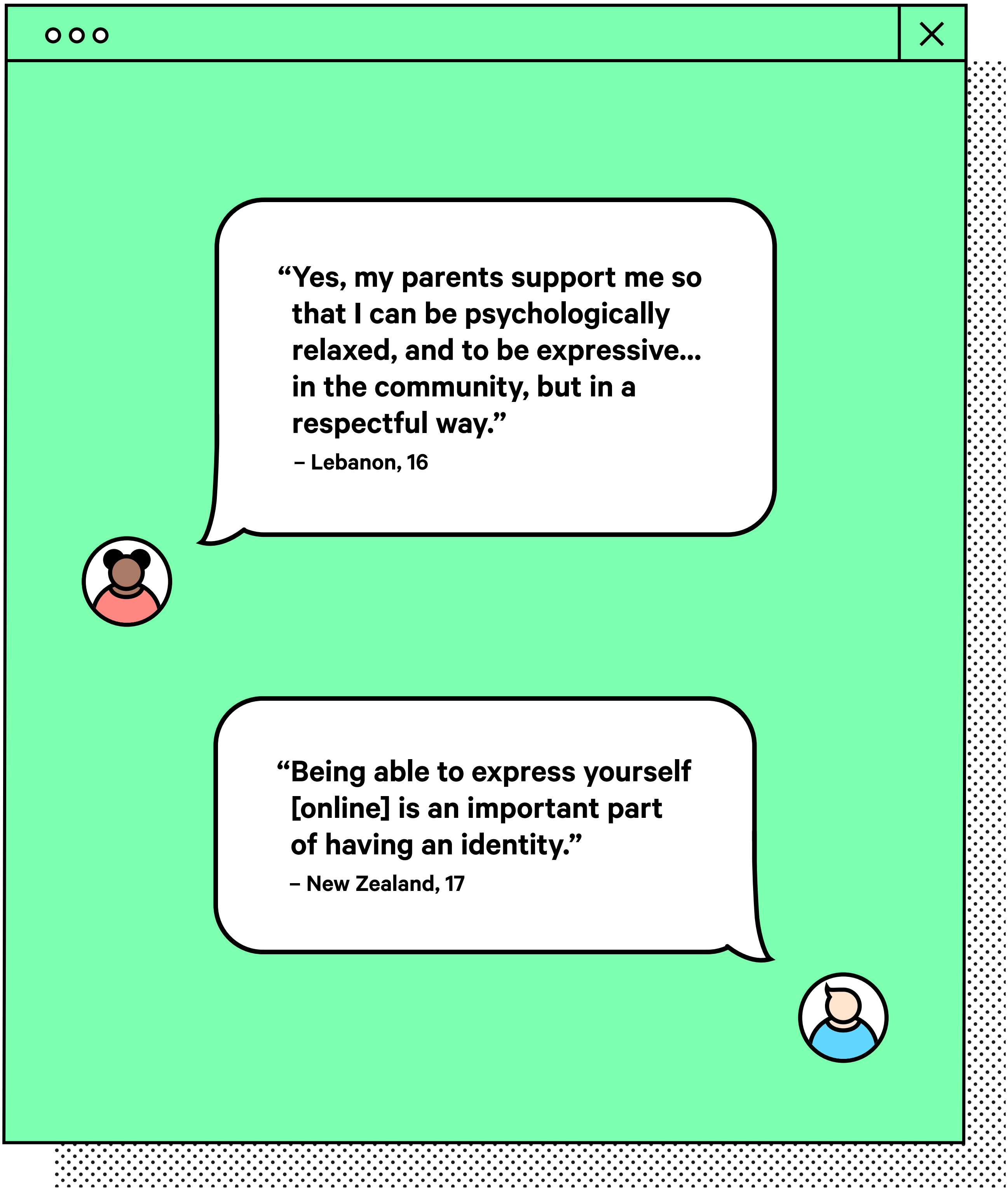
11. **INTERPOL's Crimes Against Children Unit**[186]
INTERPOL works to address those crimes against children that have an international dimension. To help trace missing children, they issue Yellow Notices, while their human trafficking experts work alongside member countries to rescue child victims of trafficking and forced labour. The unit also blocks access to child sexual abuse material.

[185] About Us, Internet Watch Foundation.

[186] Who We Are, INTERPOL.

< PREVIOUS SECTION

NEXT SECTION >



> “Yes, my parents support me so that I can be psychologically relaxed, and to be expressive... in the community, but in a respectful way.”
>
> – Lebanon, 16

> “Being able to express yourself [online] is an important part of having an identity.”
>
> – New Zealand, 17

< PREVIOUS SECTION NEXT SECTION >

5 Corporate responsibility

The business sector, including not-for-profit organizations, affects children's rights directly and indirectly in the provision of services and products relating to the digital environment. Businesses should respect children's rights and prevent and remedy abuse of their rights in relation to the digital environment. States parties have the obligation to ensure that businesses meet those responsibilities.

States parties should take measures, including through the development, monitoring, implementation and evaluation of legislation, regulations and policies, to ensure compliance by businesses with their obligations to prevent their networks or online services from being used in ways that cause or contribute to violations or abuses of children's rights, including their rights to privacy and protection, and to provide children, parents and caregivers with prompt and effective remedies. They should also encourage businesses to provide public information and accessible and timely advice to support children's safe and beneficial digital activities.

States parties have a duty to protect children from infringements of their rights by business enterprises, including the right to be protected from all forms of violence in the digital environment. Although businesses may not be directly involved in perpetrating harmful acts, they can cause or contribute to violations of children's right to freedom from violence, including through the design and operation of digital services. States parties should put in place, monitor and enforce laws and regulations aimed at preventing violations of the right to protection from violence, as well as those aimed at investigating, adjudicating on and redressing violations as they occur in relation to the digital environment.

States parties should require the business sector to undertake child rights due diligence, in particular to carry out child rights impact assessments and disclose them to the public, with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children. They should take appropriate steps to prevent, monitor, investigate and punish child rights abuses by businesses.

In addition to developing legislation and policies, States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children. They should require such businesses to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the child. They should also require the provision of age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service.

Source: General comment No. 25 (2021), paras 35-39[187]

[187] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

Objective:

To promote child-centred design, minimum standards, industry agreements, adoption of best practice and cultural awareness and resourcing of child online safety through regulation and frameworks that relate to corporate responsibility.

Model policy text:

To ensure a holistic approach to child online safety, each of the steps below is necessary.

5a. Implement safety, rights, and ethics by design
Standards and codes of practice should be developed which require product designers, manufacturers and service providers to uphold children's rights and to contribute to children's online safety and security. Terms and conditions should reflect the child's best interests. Among other things, standards and codes of practice will aim to prevent children from being offered harmful or inappropriate content or contact; to protect children's online privacy on the system- or device-level; and to address security concerns raised by the Internet of Things – connected toys and services with a streaming function – to ensure that private companies have considered, through a Child Impact Assessment, a risk and mitigation process that leads to offering children an age-appropriate service.

5b. Introduce minimum standards[188]
Industry has a responsibility to ensure that children are afforded protection online. This means creating a safe and accessible online space for children, not just preventing access to harmful content. Businesses will be required to show what procedures and special considerations they have undertaken to ensure child safety and respect for children's rights – using the 4C risk framework[189] – as they develop and establish their online services.[190] A code should be created by the lead ministry or agency, overseen by the Steering Committee. These standards will be mandatory and enforceable.

5c. Application of age-rating classification
The application of consistent age-rating classification of commercial content, public service media and games and activities online offers a transparent and effective approach to managing content and services that impact children. This may be required for relevant goods and services and for content that is suitable for different age ranges. Age assurance or creating adult-only spaces will be required for prohibited content or activities that are not suitable for children. This may include providing content filters to block unwanted content.[191]

5d. Introduce moderation and reporting systems
Mechanisms to identify upsetting or unsuitable content will be required of the service providers, and transparent and robust monitoring systems must be in place for all online services, including the provision of takedown mechanisms. A free public hotline will be available for reporting and accessing specialist support and advice. Reporting mechanisms should be easily accessible for children. Flagging systems should be considered as an additional tool. ▶

[188] See, for example, Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, GOV.UK, 2020.

[189] See section on Mitigating Risk and Harm.

[190] Children's Rights in Impact Assessments, United Nations Children's Fund, 2013.

[191] But how do they know it is a child?, 5Rights Foundation, 2021.

< PREVIOUS SECTION   NEXT SECTION >

5e. Ensure protection of children from commercial pressures
Efforts to protect children from commercial pressures will include: promoting age-appropriate design; disabling targeted advertising and third-party sharing; and raising awareness of the context in which children grow up. Products and services that enhance children's rights and safety online may be certified, and action may be taken against developers of products and services that violate these values.

5f. Ensure that child-centred design principles are introduced to minimise child online safety risks
This includes, for example, the potential for introducing adult strangers to children, or targeted advertising for gambling or the recommendation of harmful content. Child online safety needs to be embedded at the design stage to prevent issues arising further down the line.

Roadmap to achieving the objective:

A **Implement safety, rights, and ethics by design**

Standards and codes of practice will be developed which require product designers, manufacturers and service providers to uphold children's rights and to contribute to children's online safety and security. Terms and conditions should reflect the child's best interests. Among other things, standards and codes of practice will aim to prevent children from being offered harmful or inappropriate content or contact; to protect children's online privacy on the system- or device-level; and to address security concerns raised by the Internet of Things – connected toys and services with a streaming function – to ensure that private companies have considered, through a Child Impact Assessment, a risk and mitigation process that leads to offering children an age-appropriate service.

If yes, provide details:

If no, it will help to:

1. Identify the regulatory or legal opportunity to house a safety-by-design code of conduct.
2. Identify a regulatory authority or body with the resources and expertise to drive compliance and enforcement where necessary.
3. Develop a safety/rights-by-design framework – there are many examples of this, i.e Safety by Design,[192] from which to build or borrow.
4. Ensure that all stakeholders are aware of the processes (both technological and governance) necessary to deliver the framework.
5. Undertake regular landscape review of emerging harms and the efficacy of frameworks to ensure they keep pace with innovation and business practice.

[192] Safety by Design, eSafety Commissioner, 2018.

< PREVIOUS SECTION NEXT SECTION >

B Introduce minimum standards[193]

Industry has a responsibility to ensure that children are afforded protection online. This means creating a safe and accessible online space for children, not just preventing access to harmful content. Businesses will be required to show what procedures and special considerations they have undertaken to ensure child safety and respect for children's rights – using the 4C risk framework[194] – as they develop and establish their online services.[195]A code should be created by the lead ministry or agency, overseen by the Steering Committee. These standards will be mandatory and enforceable.

If yes, provide details:

If no, it will help to:

1. Introduce minimum standards in areas covered by the framework above. Identify relevant models[196] from other countries or regions.
2. Check minimum standards cover the following areas: age assurance, moderation, terms or community rules, automated decision making, and advertising. See Supportive tool 1 (page no. 109).

[193] See, for example, Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, GOV.UK, 2020.

[194] See section on Risk and Harm.

[195] Children's Rights In Impact Assessments, United Nations Children's Fund, 2013.

[196] See, for example Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, GOV.UK, 2020.

< PREVIOUS SECTION NEXT SECTION >

C Application of age-rating classification

The application of consistent age rating classification of commercial content, public service media and games and activities online offers a transparent and effective approach to managing content and services that impact children. This may be required for relevant goods and services for content that is suitable for different age ranges. Age assurance or creating adult-only spaces will be required for prohibited content or activities that are not suitable for children. This may include providing content filters to block unwanted content.[197]

If yes, provide details:

If no, it will help to:

1. Find an appropriate age-rating service. Many countries already have age-rating on commercial films[198] and/or toys and it is possible to use those same criteria when applying them to online material and activity.
2. Extend the requirement to age rate content and activity to digital spaces, including apps.
3. Ensure that an appropriate body has oversight of disputes and failure to comply.

D Introduce moderation and reporting systems

Mechanisms to identify upsetting or unsuitable content will be required of the service providers, and transparent and robust monitoring systems must be in place for all online services, including the provision of takedown mechanisms. A free public hotline will be available for reporting and accessing specialist support and advice. Reporting mechanisms should be easily accessible for children. Flagging systems should be considered as an additional tool.

If yes, provide details:

If no, it will help to:

1. Establish minimum standards, as set out in process A.
2. Consider which agency will be responsible for a public hotline.
3. Consult with experts to ensure mechanisms will be accessible for children.

[197] But how do they know it is a child? 5Rights Foundation, 2021.

[198] See for example the British Board of Film Classification.

< PREVIOUS SECTION NEXT SECTION >

E Ensure protection of children from commercial pressures

Efforts to protect children from commercial pressures will include: promoting age-appropriate design; disabling targeted advertising and third-party sharing; and raising awareness of the context in which children grow up. Products and services that enhance children's rights and safety online may be certified, and action may be taken against purveyors of products and services that violate these values.

If yes, provide details:

If no, it will help to:

1. Identify existing laws and regulations that pertain to commercial engagement with children: child protection, consumer law and children's rights all have restrictions on how you can engage commercially with children – as do particular sectors such as health or education.
2. Harmonise guidance to ensure that it extends explicitly to digital products and services.

F Ensure that child-centred design principles are introduced to minimise child online safety risks

This includes, for example, the potential for introducing adult strangers to children, or targeted advertising for gambling or the recommendation of harmful content. Child online safety needs to be embedded at the design stage to prevent issues arising further down the line.

If yes, provide details:

If no, it will help to:

Consider safety by design standards[199] in specific areas that affect children unintentionally, such as adult gambling, financial services, pornography, or other places where children are not anticipated to visit online.

[199] But how do they know it is a child? 5Rights Foundation, 2021.

< PREVIOUS SECTION NEXT SECTION >

How this aligns with foundational documents:

> **General state regulatory and policy functions**
>
> **In meeting their duty to protect, States should:**
>
> **(a) enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically to assess the adequacy of such laws and address any gaps;**
>
> **(b) ensure that other laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights;**
>
> **(c) provide effective guidance to business enterprises on how to respect human rights throughout their operations;**
>
> **(d) encourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts.**
>
> Source: United Nations Guiding Principles on Business and Human Rights 2011, section 3[200]

> **States parties should make the best interests of the child a primary consideration when regulating advertising and marketing addressed to and accessible to children. Sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate gender or racial stereotypes.**
>
> General comment No. 25 (2021), para 41[201]

> **States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children.**
>
> Source: General comment No. 25 (2021), para 42[202]

Supportive tools:

1. Steps for designing digital products and services with children's rights in mind

5Rights Foundation and the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) have created a standard which introduces practical steps that companies can follow to design digital products and services that are age-appropriate. It introduces a series of processes that companies can follow to put young people's needs at the heart of design.

[200] Guiding Principles on Business and Human Rights, Office of the United Nations High Commissioner for Human Rights 2011.

[201] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[202] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

Other resources for reference:

1. An example of young people’s thoughts on corporate responsibility

The young people that 5Rights spoke to wanted to see the following from companies:

- Consistent community rules across platforms
- Clear timelines for reporting
- The ability to tell victims what happened to their bully
- Better content labelling
- Easy ways to take content down
- A ban on spreading abuse
- Pop-ups that point to good behaviours and encourage use of high-privacy settings
- A clear end point to complaint processes
- Policies written in plain language

2. Guidance from UN Children’s Rights and Business Principles about private sector accountability[203]

The private sector also has responsibilities for child online safety, and this should be made clear in relevant policy areas. Some areas, such as cyberbullying, CSEA, financial fraud etc have specific frameworks to support child online safety but there are also overarching frameworks for corporate responsibility.

The Children’s Rights and Business Principles ask all business to:

□ Meet their responsibility to respect children’s rights and commit to supporting the human rights of children.

□ Contribute towards the elimination of child labour, including in all business activities and business relationships.

□ Provide decent work for young workers, parents and caregivers.

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

□ Ensure that products and services are safe, and seek to support children’s rights through them.

□ Use marketing and advertising that respect and support children’s rights.

□ Respect and support children’s rights in relation to the environment and to land acquisition and use.

□ Respect and support children’s rights in security arrangements.

□ Help protect children affected by emergencies.

□ Reinforce community and government efforts to protect and fulfil children’s rights.

[203] Obligations and Actions on Children’s Rights and Business, International Commission of Jurists and United Nations Children’s Fund, 2015.

< PREVIOUS SECTION NEXT SECTION >

3. **General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights**[204]
This is the UN Committee on the Rights of the Child's guidance about the obligations States have regarding the impact of business activities and operations on children's rights.

4. **Children's Rights and Business Explained**[205]
This is a reader-friendly version of the Committee on the Rights of the Child's General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights.

5. **Guiding Principles on Children's Rights and Business**[206]
Developed by UNICEF, UN Global Compact and Save the Children, this is a comprehensive set of principles to guide companies on the full range of actions they can take in the workplace, marketplace and community to respect and support children's rights.

6. **Obligations and Actions on Children's Rights and Business**[207]
This is a practical guide for States on how to implement the United Nations Committee on the Rights of the Child's General comment No. 16 (2013).

7. **IEEE 2089-2021 Standard for Age-Appropriate Digital Services Framework**[208]
5Rights Foundation and the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) have created a standard which introduces practical steps that companies can follow to design digital products and services that are age-appropriate.

8. **UNICEF Guide to Using the Child Online Safety Assessment Tool – Empowering technology companies to promote a safe online environment for children**[209]
This is UNICEF's guidance on using their Child Online Safety Assessment Tool, to support businesses in preparing for and completing an assessment of their impacts related to children. It describes the purpose, background and functions of the Child Online Safety Assessment Tool, and offers detailed instructions and advice on how to use the tool.

9. **Child Safety Online – A Practical Guide for Providers of Social Media and Interactive Services**[210]
This is the UK Government's guide for social media providers to make their platforms safer for users, built on the safety framework of the ICT Coalition for Children Online – a European industry initiative.

[204] General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, United Nations Convention on the Rights of Child, 2013.

[205] Children's Rights and Business Explained, United Nation's Childrens Fund and Save the Children, 2015.

[206] Children's Rights and Business Principles, United Nations Children's Fund, United Nations Global Compact and Save the Children, 2013.

[207] Obligations and Actions on Children's Rights and Business, International Commission of Jurists and United Nations Children's Fund, 2015.

[208] IEEE 2089-21 Standard for Age-Appropriate Digital Services Framework, IEEE SA, 2021.

[209] Guide to Using the Child Online Safety Assessment Tool, United Nations Children's Fund, 2016.

[210] Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services, UK Department for Digital, Culture, Media & Sport, 2016.

< PREVIOUS SECTION NEXT SECTION >

10. **5Rights Foundation report – But How Do They Know It Is a Child**[211]
This is 5Rights Foundation's report addressing the debate on age verification, estimation and assurance.

11. **Italian Code on Cyberbullying**[212]
This is the Italian Government's formal code on cyberbullying (in Italian).

12. **Financial Coalition Against Child Pornography**[213]
This report describes methods used by some Financial Coalition Against Child Pornography members in their application and verification process, and thereafter to detect CSAM and prevent the establishment or maintenance of merchant accounts related to the commercial distribution and sale of CSAM.

13. **Commercial Sexual Exploitation of Children Online 2015**[214]
This report from the European Financial Coalition against Commercial Sexual Exploitation of Children Online is an update to the Strategic Assessment of Commercial Sexual of Children Online published in October 2013, in the framework of the European Financial Coalition. In addition to presenting the 2013 facts and figures, it also looks at other essential factors in this area.

14. **Child Online Safety Universal Declaration**[215]
This is the Broadband Commission's Declaration, which aims to align all relevant stakeholders on the common mission of championing the cause of protection of children online.

15. **UNICEF Albania Trilogy of Promising Practice**[216]
This is a case study from Albania. Four of the top five internet and communications companies have engaged in a participative process to develop industry guidelines which have been released by the National Authority for Electronic Certification and Cybersecurity.

16. **OECD Guidelines for Digital Service Providers**[217]
These Guidelines seek to complement the Recommendation of the Council on Children in the Digital Environment [FOOTNOTE 2] and support Digital Service Providers, when they take actions that may directly or indirectly affect children in the digital environment, in determining how best to protect and respect the rights, safety, and interests of children.

[211] But how do they know it is a child?, 5Rights Foundation, 2021.

[212] Provisions for the protection of minors for the prevention and contrast of the phenomenon of cyberbullying, Gazzetta Ufficiale, 2017.

[213] Internet Merchant Acquisition and Monitoring Sound Practices to Help Reduce the Proliferation of Commercial Child Pornography, International Centre for Missing & Exploited Children, 2016.

[214] Commercial Sexual Exploitation of Children Online, Europol, 2015.

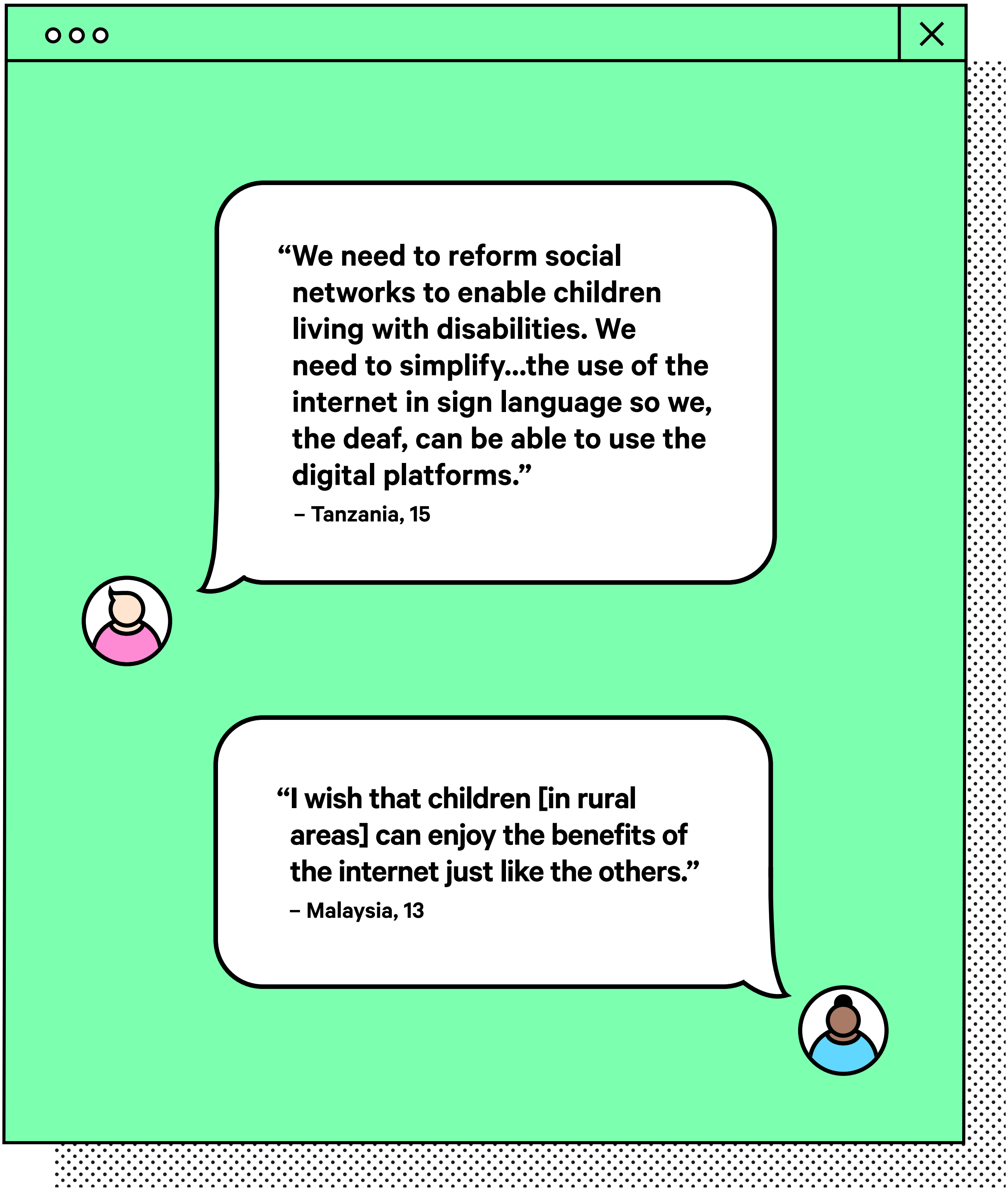
[215] Child Online Safety Universal Declaration, Broadband Commission, 2019.

[216] Programming for Children's Protection Online in Albania, United Nations Children's Fund, 2020.

[217] OECD Guidelines for Digital Service Providers, OECD, 2021.

< PREVIOUS SECTION

NEXT SECTION >



"We need to reform social networks to enable children living with disabilities. We need to simplify...the use of the internet in sign language so we, the deaf, can be able to use the digital platforms."
– Tanzania, 15

"I wish that children [in rural areas] can enjoy the benefits of the internet just like the others."
– Malaysia, 13

< PREVIOUS SECTION

NEXT SECTION >

6 Training

> **Professionals working for and with children and the business sector, including the technology industry, should receive training that includes how the digital environment affects the rights of the child in multiple contexts, the ways in which children exercise their rights in the digital environment and how they access and use technologies. They should also receive training on the application of international human rights standards to the digital environment. States parties should ensure that pre-service and in-service training relating to the digital environment is provided for professionals working at all levels of education, to support the development of their knowledge, skills and practice.**
>
> Source: General comment No. 25 (2021), para 33[218]

Objective:

To ensure that all those involved with services relating to children, including government, law enforcement, justice, health and wellbeing, politicians, and civil servants, as well as those designing technology, have a good understanding of child online safety and children's best interests.

Model policy text:

To ensure a holistic approach to child online safety, each of the steps below is necessary.

6a. Provide training, skills development and mentoring for all involved in child online safety
From first responders to judges, all actors in the law enforcement chain, and professionals who work with children in other settings like education or health, must be aware of child online safety. They should be offered comprehensive training, including on how child online safety relates to their particular role, how to understand offending behaviour, and how to provide access to victim support.

6b. Provide specialised training for psycho-social support and identification of signs of the full range of child online safety issues
To be effective, relevant practitioners must be provided with child online safety training, training on safeguarding and child protection policies, and training on child and family counselling. Child online safety awareness should be incorporated into existing frameworks for child protection. Professionals working with children in education, health, community and other settings should be trained to recognise the signs and symptoms of child online safety issues.

6c. Build tertiary education schemes
Child online safety sessions should form a mandatory part of teaching, social work, health work, psychology, and other relevant degree programmes in public and private universities or education institutions. There is a need for regular review of the effectiveness of this teaching in light of advances in child online safety training and emerging issues. Curricula should cover all aspects of child online safety as laid out in this policy. ▶

[218] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

6d. Encourage professional development

Continuing education programmes on child online safety and child safeguarding for professionals working in relevant fields will be established, regularly reviewed and updated to keep pace with emerging technologies, and to address new barriers and concerns as they become apparent.

Roadmap to achieving the objective:

A Provide training, skills development and mentoring for all involved in child online safety

From first responders to judges, all actors in the law enforcement chain, and professionals who work with children in other settings like education or health, must be aware of child online safety. They should be offered comprehensive training, including on how child online safety relates to their particular role, how to understand offending behaviour, and how to provide access to victim support.

If yes, provide details:

If no, it will help to:

1. Identify all the necessary professions and contacts who may need training in child online safety. Supportive tool 1 below may assist with this (see page no. 119).
2. Review existing training programmes and consider at what point and to what level of detail child online safety training is required (see Resources below).
3. Commission or update existing child online safety training relevant to the field. These materials may be shared across disciplines to ensure high quality training.
4. Ensure qualification in any field is subject to successful completion.
5. Ensure training materials are regularly updated and cover all aspects of a child's online life: content, contact, conduct and commercial risks.
6. Consider how to involve the voice and opinion of children and young people in training.[219]

[219] See for example, The Lundy Model of Child Participation, European Commission, 2007.

< PREVIOUS SECTION NEXT SECTION >

B Provide specialised training for psycho-social support and identification of signs of the full range of child online safety issues

To be effective, relevant practitioners must be provided with child online safety training, training on safeguarding and child protection policies, and training on child and family counselling. Child online safety awareness should be incorporated into existing frameworks for child protection. Professionals working with children in education, health, community and other settings should be trained to recognise the signs and symptoms of child online safety issues, understand offending behaviour, and how to provide access to victim support.

If yes, provide details:

If no, it will help to:

1. Identify those that need training for psycho-social support and CSEA.
2. Identify fully tested training, at either an international or regional level (see Other resources for reference 1-4 below).
3. Ensure funding resources and time are a priority for CSEA training.
4. Identify when and how training will be delivered, reviewed and improved.
5. Consider how to involve the voice and opinion of children and young people in training.[220]
6. Build KPIs for workforce training that must be evaluated and reported regularly.

[220] See for example, The Lundy Model of Child Participation, European Commission, 2007.

< PREVIOUS SECTION NEXT SECTION >

C Build tertiary education schemes

Child online safety sessions should form a mandatory part of teaching, social work, health work, psychology, and other relevant degree programmes in public and private universities or education institutions. There is a need for regular review of the effectiveness of this teaching in light of advances in child online safety training and emerging issues. Curricula should cover all aspects of child online safety as laid out in this policy.

If yes, provide details:

If no, it will help to see Other resources for reference 1 (below) for examples.

D Encourage professional development

Continuing education programmes on child online safety and child safeguarding for professionals working in relevant fields will be established, regularly reviewed and updated to keep pace with emerging technologies, and to address new barriers and concerns as they become apparent.

If yes, provide details:

If no, it will help to:

1. Ensure training is available throughout the life cycle of a professional's working life, and respond to changes both in the digital world and in the roles of professionals.
2. Identify opportunities for further training.
3. Build training curricula that support more detailed or 'top-up' learning (see Other resources for reference 1-4 below).
4. Consider how to involve the voice and opinion of young people in training.[221]

[221] See for example, The Lundy model of chid participation, European Commission, 2007.

< PREVIOUS SECTION NEXT SECTION >

How this aligns with foundational documents:

> **States parties should address the ways in which uses of digital technologies may facilitate or impede the investigation and prosecution of crimes against children and take all available preventative, enforcement and remedial measures, including in cooperation with international partners. They should provide specialised training for law enforcement officials, prosecutors and judges regarding child rights violations specifically associated with the digital environment, including through international cooperation.**
>
> Source: General comment No. 25 (2021), para 47[222]

[222] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

Supportive tools:

1. A checklist of professions that may benefit from specific training, and topics to address

This is designed to help you identify if existing training is appropriate and relevant for professionals in your jurisdiction, and to identify where the gaps are. This is part of achieving Process A ('Provide training, skills development and mentoring for all involved in child online safety').

Profession	Training for all child online safety issues, and the 4Cs of risk	Training on safeguarding and safeguarding policies	Recognising child online safety issues	Understanding offender behaviour and rehabilitation	Counselling	Victim support
Judges	✎ *[identify existing training, or identify gaps]*					
Law enforcement						
Social workers						
Health workers						
Teachers						
Workers in community settings						
Psychologists						
Others						

< PREVIOUS SECTION NEXT SECTION >

Other resources for reference:

There are many examples of training modules available online for different groups of professionals. Induction, tertiary and ongoing training should be provided to a wide range of professionals, including teachers/educators, law enforcement, justice sector workers, social and youth workers, healthcare professionals, parliamentarians, civil servants, technologists (including computer programmers, UX designers and those responsible for governance) and regulators in the relevant fields.

1. **Resources for teachers, social workers and youth workers**
   See NSPCC Online Safety Training. Anyone who works with children and young people needs to know what to do if a child comes to them about something concerning that they have seen online. This training is designed to help professionals feel confident in keeping children safer online.[223]

2. **Resources for healthcare professionals**
   eIntegrity's online child protection training for healthcare professionals (Safeguarding Children and Young People) covers the knowledge and competencies needed by health and social care professionals to safeguard the welfare of children. It has been developed by a consortium of professional bodies, led by the Royal College of Paediatrics and Child Health.[224]

   This online safeguarding course is mapped to the UK framework for training in this area, the intercollegiate document Safeguarding Children and Young People: Roles and Competencies for Health Care Staff (2019).[225] However, the themes are relevant to health and social care professionals globally.[226]

3. **Resources for law enforcement[227]**
   ICMEC provides a range of different training opportunities and courses such as:

   □ Essentials of Technology-Facilitated Crimes Against Children

   □ Advanced Online Exploitation Investigations

   □ Advanced Technologies

   □ Fundamentals of Responding to Missing Children.

[223] Introduction to safeguarding and child protection training, National Society for the Prevention of Cruelty to Children.

[224] Online child protection training for healthcare professionals, eIntegrity.

[225] Safeguarding children and young people – roles and competencies, Royal College of Paediatrics and Child Health, 2019.

[226] Online child protection training for healthcare professionals, eIntegrity.

[227] Building global capacity to keep children safer from harm, International Centre for Missing & Exploited Children, 2015 and ICMEC Resources, International Centre for Missing & Exploited Children.

< PREVIOUS SECTION

NEXT SECTION >

4. **Gender-Based Violence in Namibia: An exploratory assessment and mapping of GBV response services in Windhoek, 2016**[228]
Namibia's Gender-Based Violence (GBV) Protection Unit (GBVPU) and Child Witness Training programmes provide training to police investigators, prosecutors, magistrates and social workers (child protection workforce) to ensure improved end-to-end support for victims. The GBVPU is disability-accessible, with a child-friendly video interviewing room, and is guided by Standard Operating Procedures for GBV/VAC.

5. **Resources for the justice sector**[229]
The Council of Europe's EndOCSEA project provides training for judges and prosecutors on CSEA.

6. **General resources**
The Queensland Family and Child Commission has produced a Protecting Children Online Module.[230]

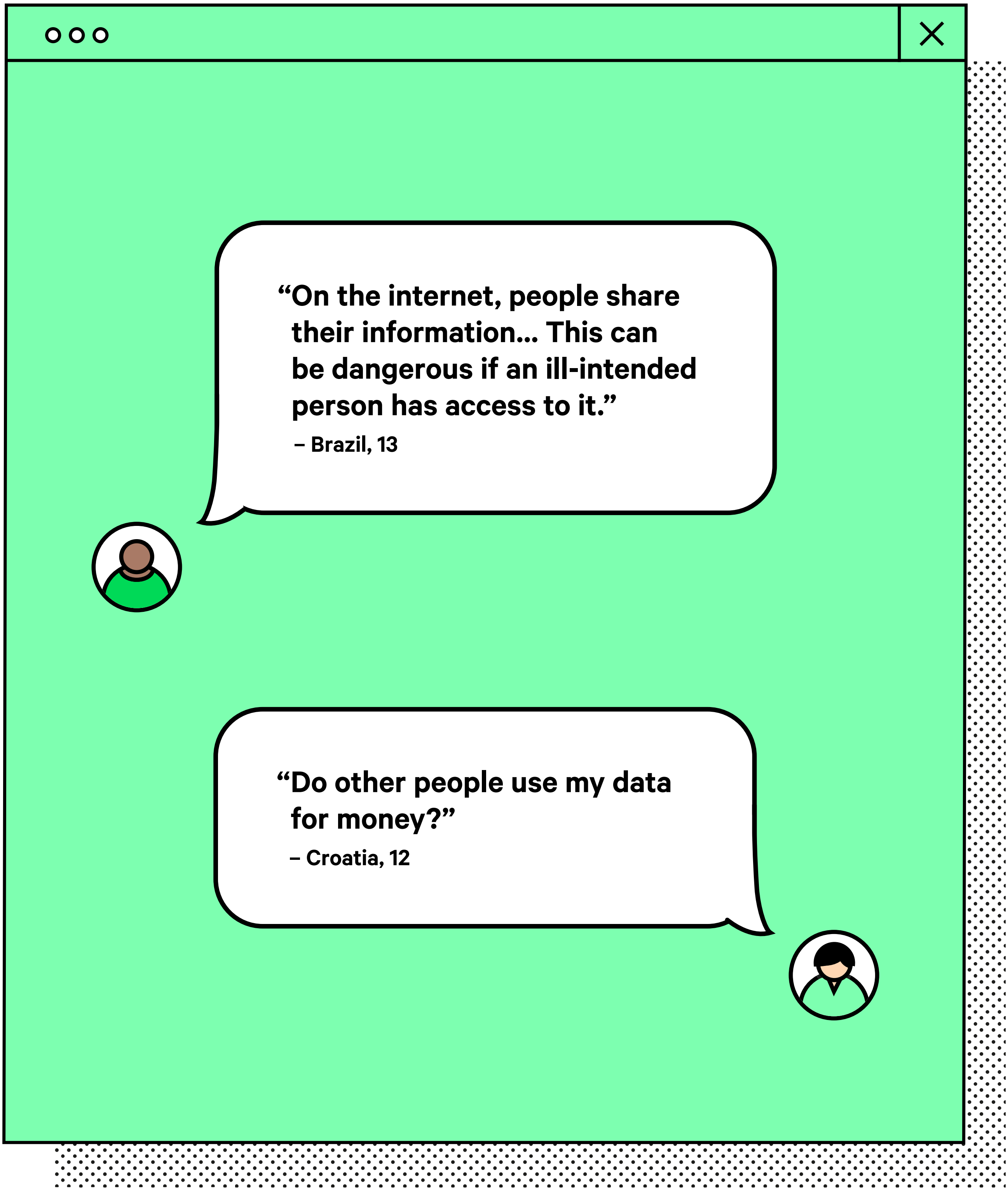
[228] Gender-based Violence in Namibia: An exploratory assessment and mapping of GBV response services in Windhoek, Victims 2 Survivors and UNAIDS, 2016.

[229] End Online Child Sexual Exploitation and Abuse, Council of Europe, 2021.

[230] Protecting children online module, Queensland Family & Child Commission, 2022.

< PREVIOUS SECTION

NEXT SECTION >



"On the internet, people share their information… This can be dangerous if an ill-intended person has access to it."
– Brazil, 13

"Do other people use my data for money?"
– Croatia, 12

< PREVIOUS SECTION NEXT SECTION >

7 Education

> **States parties should provide and support the creation of age-appropriate and empowering digital content for children in accordance with children's evolving capacities and ensure that children have access to a wide diversity of information, including information held by public bodies, about culture, sports, the arts, health, civil and political affairs and children's rights.**
>
> **States parties should encourage the production and dissemination of such content using multiple formats and from a plurality of national and international sources, including news media, broadcasters, museums, libraries and educational, scientific and cultural organizations. They should particularly endeavour to enhance the provision of diverse, accessible and beneficial content for children with disabilities and children belonging to ethnic, linguistic, indigenous and other minority groups. The ability to access relevant information, in the languages that children understand, can have a significant positive impact on equality.**
>
> Source: General comment No. 25 (2021) paras 51 and 52[231]

Objective:

To promote the positive use of digital technology as a source of entertainment, information and learning for children in a safe environment.

Model policy text:

To ensure a holistic approach to child online safety, each of the steps below is necessary.

7a. Designate child protection leads
Each school is to designate a child protection lead.[232] Each lead is to be provided with training on child protection procedures and child online safety-specific training. Leads will be responsible for ensuring that child online safety policies (including safeguarding procedures and anonymous reporting systems) are adopted, enacted and enforced in schools. The child protection lead will be the point of contact for concerns relating to child protection and child online safety, and will pass on reported harms to the relevant authorities. Leads should also facilitate intervention plans, to protect children against the full range of harms.

7b. Promote accessible digital education
Promote content, including peer-to-peer programmes, that are designed and shown to help children develop digital skills and empower children to build respectful communities that support child online safety. Digital education should be holistic and should cover data and media literacy, alongside safeguarding issues – in particular issues of sexuality and consent. Education should also be extended to parents/carers to support their role in promoting child online safety. ▶

[231] General comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, United Nations Committee on the Rights of the Child, 2021.

[232] This could be someone from a school safety committee, an educator or it could be someone in a village or community child protection committee where schools are represented.

7c. Promote educational content

As digital adoption becomes widespread, pupils and teachers will be taught the necessary skills for interacting with digital systems to fully benefit from curriculum content, both in local and international languages.

7d. Promote data literacy

A programme of data literacy will be introduced across the school curriculum. The programme will educate children on the way their data may be used and will provide a basic understanding of the data economy. It will: emphasise and encourage the positive, autonomous and creative use of digital technologies by children; clearly define the risks, benefits, and social outcomes of using technology; and aim to ensure that protective and preventative measures are broadly disseminated, understood and applied. Data literacy education should make clear the range of stakeholders responsible for online safety.

7e. Promote critical thinking

Education for children and parents/carers on critical thinking and awareness of the risks of online disinformation should be incorporated into digital literacy education. This should include wider education to promote understanding and awareness of human rights, in particular children's rights, and the way they work online and offline.[233]

7f. Introduce formal child online safety procedures in schools

Child online safety training must form a mandatory part of teaching degrees, at both primary and secondary school level, as well as a focus of ongoing in-service training. All teachers must complete mandatory training on child online safety, be aware of school policy in relation to child online safety, and deliver child online safety lessons to students. All schools must appoint a child online safety lead to champion child online safety standards and take responsibility for enforcing school policy on child online safety.

[233] See Article 29 of the Convention on the Rights of the Child, and relevant sections of the general comment.

< PREVIOUS SECTION NEXT SECTION >

Roadmap to achieving the objective:

A Designate child protection leads

Each school is to designate a child protection lead.[234] Each lead is to be provided with training on child protection procedures and child online safety-specific training. Leads will be responsible for enacting and enforcing child protection policies (including safeguarding procedures and anonymous reporting systems) in schools. They will be the point of contact for concerns relating to child protection and child online safety, and will pass on reported harms to the relevant authorities. Leads should also facilitate intervention plans, to protect children against the full range of harms.

If yes, provide details:

If no, it will help to:

1. Identify the school's existing child protection and safeguarding policies and rules, and ensure they include modules on child online safety. Where none exist, search for best practice. See Other resources 1-6 for examples.
2. In either case, ensure that preparation for each school year includes up-to-date child protection and safeguarding measures, addressing all teachers with an overview of child safety issues. See Other resources 2 for online courses available to frontline workers.

[234] This could be someone from a school safety committee, an educator or it could be someone in a village or community child protection committee where schools are represented.

< PREVIOUS SECTION NEXT SECTION >

B Promote accessible digital education

Promote content, including peer-to-peer programmes, that are designed and shown to help children develop digital skills and empower children to build respectful communities that support child online safety. Digital education should be holistic, and should cover data and media literacy, alongside issues of sexuality and consent. Child protection and safeguarding education should also be extended to parents/carers to support their role in promoting child online safety.

If yes, provide details:

If no, it will help to:

1. Ensure digital literacy covers the full gamut of online experience, not just safety issues, as many children who dislike e-safety are very open to a broader understanding of opportunity and risk. Look at the DQ model (see Other resources 3) of the areas that should be covered (see Resources below), and ensure that any areas that discuss risk cover all the 4Cs (see Identifying risks and mitigating harm section).
2. Ensure that sex education, sexuality and consent are taught in the context of the digital world, to ensure that children have maximum agency over related issues that may come up online.
3. Identify digital literacy programmes in an appropriate language or that are available for translation as needed.[235]
4. Ensure digital literacy for parents/carers is fully aligned with digital literacy for children. Parental resources should be positive and well-rounded and not cause undue panic about the digital world or encourage drastic measures against children.[236]
5. Check for technology companies offering free digital literacy programmes for both children and adults. These are often very well developed and very effective – but fail to identify the commercial risks and harms of the tech itself. If the local solution is to use these programmes, check that they cover all aspects of risk, including those created by the programmes themselves.

[235] See for example Digital Literacy, International Telecommunication Union.

[236] See for example Media and Digital Literacy: Resources for Parents, The George Lucas Educational Foundation, 2012.

< PREVIOUS SECTION NEXT SECTION >

7 Education

C **Promote educational content**

As digital adoption becomes widespread, pupils and teachers will be taught the necessary skills for interacting with digital systems to fully benefit from curriculum content, both in local and international languages.

If yes, provide details:

If no, it will help to:

1. Identify good educational content that relates to the curriculum or the school's extracurricular activities.
2. Ensure that the terms of use are appropriate for the privacy and security of pupils.
3. Make sure that all pupils, regardless of gender, disability and socioeconomic status, are able to access the resources: this may require consideration of connectivity, affordability (including data) and access to suitable devices.
4. Check resources from reputable institutions – for example, universities, schools, NGOs – offered in a wide variety of subjects and resources. For some subjects, it may be better to consider the cost of translating or using existing materials rather than creating materials from scratch; in other cases, commissioning or identifying material in local languages, that covers local culture or histories, may be an important investment.
5. Consider that the wide availability of online materials should allow for an extension of subject matter beyond the skilled teaching available locally – however, it is still the case that a trained classroom teacher offers a qualitatively different experience to online learning.

< PREVIOUS SECTION NEXT SECTION >

D Promote data literacy

A programme of data literacy will be introduced across the school curriculum. The programme will educate children on the way their data may be used and will provide a basic understanding of the data economy. It will: emphasise and encourage the positive, autonomous and creative use of digital technologies by children; clearly define the risks, benefits, and social outcomes of using technology; and aim to ensure that protective and preventative measures are broadly disseminated, understood and applied. Data literacy education should make clear the range of stakeholders responsible for online safety.

If yes, provide details:

If no, it will help to consider the resources and actions covered in points A-C above.

E Promote critical thinking

Education for children and parents/carers on critical thinking and awareness of the risks of online disinformation should be incorporated into digital literacy education. This should include wider education to promote understanding and awareness of human rights, in particular children's rights, and the way they work online and offline.[237]

If yes, provide details:

If no, it will help to consider the resources and actions covered in points A-C above.

[237] See Article 29 of the Convention on the Rights of the Child, and relevant sections of the General comment.

< PREVIOUS SECTION

NEXT SECTION >

F Introduce formal child online safety procedures in schools

Child online safety training must form a mandatory part of teaching degrees, at both primary and secondary school level, as well as a focus of ongoing in-service training. All teachers must complete mandatory training on child online safety, be aware of school policy in relation to child online safety, and deliver child online safety lessons to students. All schools must appoint a child online safety lead to champion child online safety standards and take responsibility for enforcing school policy on child online safety.

If yes, provide details:

If no, it will help to consider the resources and actions covered in points A-C above.

How this aligns with foundational documents:

Educate children on digital literacy as part of a strategy to ensure they can benefit from technology, free from harm. This will allow children to develop critical thinking skills that will help them to identify and understand the good and bad sides of their behaviour in the digital space. Whilst it is important to illustrate to children the harms that can occur online, this will only be effective if included as part of a broader digital literacy programme that should be age-appropriate and focus on skills and competencies. It is important to include social and emotional learning concepts within online safety education as these will support students' understanding and management of emotions to have healthy and respectful relationships, both online and offline.

Source: ITU Guidelines for policy-makers on Child Online Protection 2020[238]

Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all.

Source: Sustainable Development Goal 4[239]

[238] Guidelines for policy-makers on Child Online Protection, International Telecommunication Union, 2020.

[239] Goal 4: Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all, United Nations, 2017.

< PREVIOUS SECTION NEXT SECTION >

Supportive tools:

1. A checklist to ensure formal child online safety procedures in schools

This is designed to identify gaps in the school's child online safety procedures. It will track progress against Process F ('Introduce formal child online safety procedures in schools').

Question	Response
Is child online safety part of teacher training courses?	✎
Do all primary and secondary schools have a child online safety lead?	
Do all primary and secondary schools have a child online safety policy?	
Do all primary schools deliver online safety courses to students? a. Designate child protection leads b. Promote accessible digital education c. Promote educational content d. Promote data literacy e. Promote critical thinking f. Introduce formal child online safety procedures in schools	
Do all secondary schools deliver online safety courses to students?	

< PREVIOUS SECTION NEXT SECTION >

Other resources for reference:

1. **DQ Child Digital Readiness Kit: 8-Day Home-Based e-Learning for Children (ages 8-12) and Parents**[240]
   This is an 8-day e-learning programme, where over 8 days children learn the 8 Digital Citizenship Skills, with minimal support from parents or teachers. As children complete each Digital Citizenship Skill, parents get a DQ scorecard via email, detailing their child's progress and exposure to cyber risks. Parents also receive a digital copy of the DQ Parenting Handbook to help them improve their entire family's DQ.

2. **South Africa child online safety**[241]
   This website provides interactive guidance for educators and caregivers regarding children's online safety. Caregivers and educators are encouraged to share their strategies or school policies on the platform.

3. **National Association of School Psychologists – A Framework for Safe and Successful Schools**[242]
   This framework provides recommendations on how to enhance children and young people's physical and mental security through a strategy for safe and supportive schools.

4. **International Task Force on Child Protection – International Child Protection Standards and Expectations**[243]
   This report, prepared by the School Evaluation Committee, provides child protection evaluation requirements for accreditation and inspection agencies.

5. **Council of International Schools**[244]
   This website provides useful guidance and tools for caregivers and educators regarding children and young people's security. It offers examples of Child Protection Workshops, Mental Health and Wellbeing Workshops, and Safer Recruitment Standards, etc.

6. **NSPCC Online safety training in English**[245]
   This online course offers safety training for caregivers on how and what to look out for regarding children's online safety. It includes important issue areas such as online radicalisation and extremism, bullying, and sexual offending. ▶

[240] Global Digital Citizenship Movement for 8-12 Year-Olds, DQ Institute.

[241] Child Online Safety, Thutong Education Portal.

[242] A Framework for Safe and Successful Schools, National Association of School Psychologists, 2013.

[243] Updated Standards for Child Protection Adopted by School Evaluation Agencies, International Centre for Missing & Exploited Children, 2021.

[244] Resources, Council of International Schools.

[245] Introduction to safeguarding and child protection training, National Society for the Prevention of Cruelty to Children.

< PREVIOUS SECTION NEXT SECTION >

7. Examples of educational resources supporting child online safety

A. Sample Syllabus – Young and eSafe Curriculum from Australian Office of the eSafety Commissioner[246]
This website provides resources such as short videos and educational content to help young people learn positive online behaviours.

B. Common Sense Education Media Free Lessons to Teach Digital Citizenship to Children of All Ages[247]
This website provides free lessons to help children and young people obtain digital citizenship skills. The lessons include, for example, addressing issues such as cyberbullying and online privacy.

C. International Telecommunication Union: Online safety activity book[248]
This online safety activity book provides an introduction to the Convention on the Rights of the Child and some exercises on how to safely interact with people on the internet.

D. International Telecommunication Union: Teacher's Guide[249]
This manual contains the instructions and resources for completing these online safety exercises in a classroom setting with 9-12 year olds. The aim of the activities is to inspire students and teachers to have conversations about online safety issues and how to handle them.

E. ITU Digiworld: An example of how the ITU Guidelines on Child Online Protection can be delivered in practice[250]
This document explores how the ITU's Guidelines can be practically used to develop children's online safety.

F. Childnet International Teaching Toolkit[251]
The Step Up, Speak Up! Teaching Toolkit is a practical, interactive and scenario-based resource which addresses the issue of online sexual harassment amongst 13-17 year olds. This toolkit consists of 4 lesson plans with accompanying films, an audio story, workshops and an assembly presentation.

G. UK Guidance – Teaching online safety in school[252]
This is guidance that supports schools to teach their pupils how to stay safe online, within new and existing school subjects.

H. Council of Europe EndOCSEA Kiko and the Manymes Booklet and Video[253]
This is a storybook and video launched by the Council of Europe that provides guidance to both caregivers and young children on how to use the internet safely.

[246] Young and eSafe, Office of the eSafety Commissioner.

[247] Everything You Need to Teach Digital Citizenship, Common Sense Education.

[248] Online safety activity book - Work with Sango, International Telecommunication Union.

[249] Online safety activity book - Teacher's Guide, International Telecommunication Union.

[250] Digiworld – An example of how the ITU Guidelines on Child Online Protection can be delivered in practice, International Telecommunication Union, 2020.

[251] Teaching Toolkit, Childnet.

[252] Teaching online safety in school, Department for Education, 2019.

[253] EndOCSEA@Europe Activities - Kiko's exciting adventures continue in the digital age, Council of Europe, 2020.

< PREVIOUS SECTION NEXT SECTION >

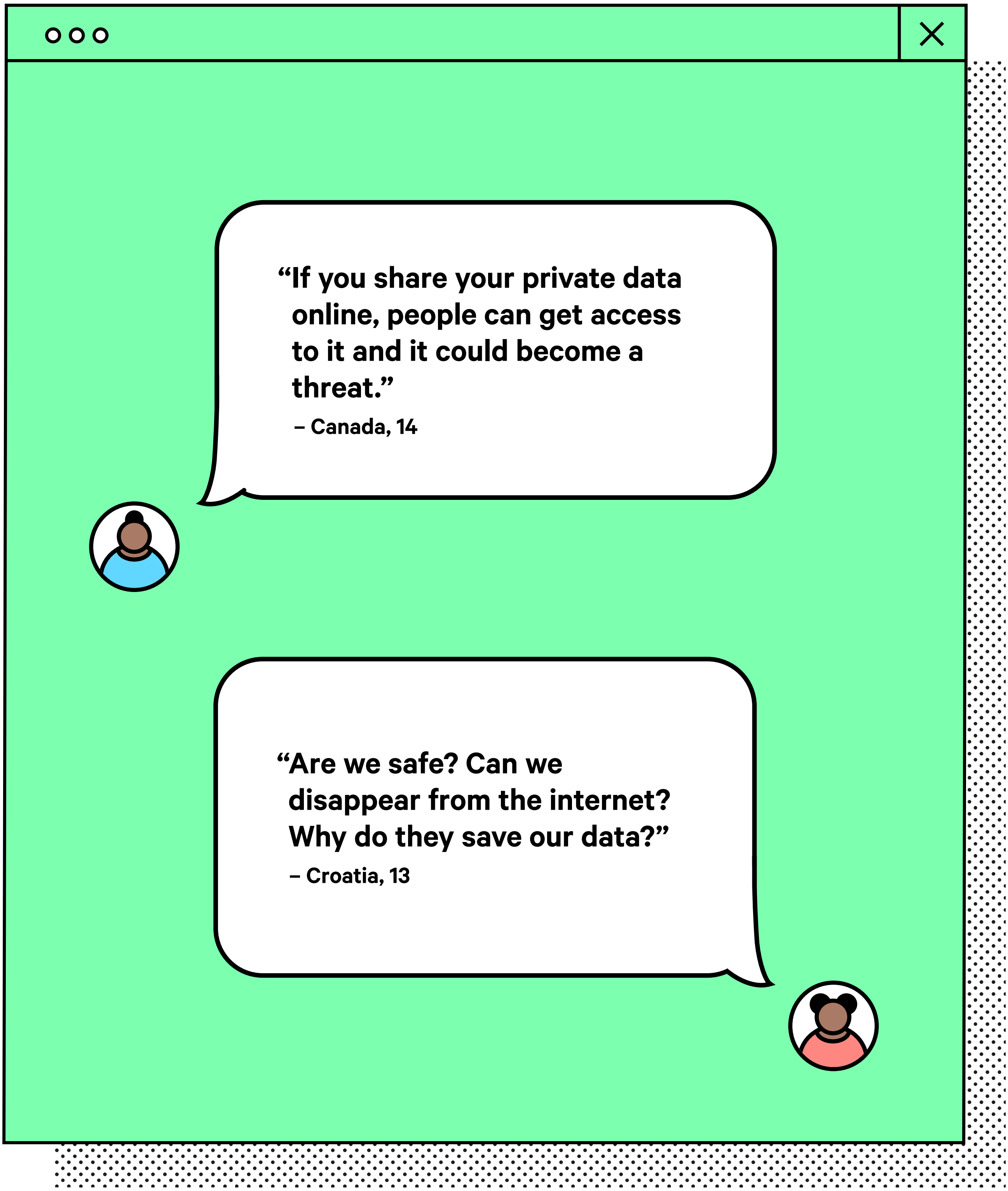
8. **Sri Lanka: WebFighter campaign**[254]
   This website provides useful guidance and tools for caregivers and educators regarding children and young people's security. It offers examples of Child Protection Workshops, Mental Health and Wellbeing Workshops, and Safer Recruitment Standards, etc.

9. **The Swipe Safe programme**[255]
   The Swipe Safe programme helps young people navigate the internet safely by educating them on potential risks, such as cyber scams, bullying or sexual abuse, and offering them strategies to protect themselves. The curriculum has been adapted by non-governmental organisations in Vietnam, Laos and Myanmar. Swipe Safe mobilises parents, young people, schools and the private sector to play an active role in children's online safety. The programme provides training for internet café owners/managers to identify and address risks and possible adverse events that might happen to children, from online to offline and vice versa. It also supports schools to develop child-friendly policies and guidance on online safety.

10. **Digital Literacy Package (DLP)**[256]
    The Ghanaian Digital Literacy Package, produced by UNICEF, has been developed to equip children with digital literacy skills and ensure they stay safe and resilient in the online space. It also has components targeting parents/carers, empowering them to support learners to stay safe online, especially in times of COVID-19, where distance learning has become the norm.

[254] Goethe Institut.
[255] ChildFund Swipe Safe, ChildFund Alliance, 2019.
[256] Digital Literacy Package (DLP), UNICEF, 2021.

< PREVIOUS SECTION NEXT SECTION >



"If you share your private data online, people can get access to it and it could become a threat."
– Canada, 14

"Are we safe? Can we disappear from the internet? Why do they save our data?"
– Croatia, 13

< PREVIOUS SECTION NEXT SECTION >

8 Public awareness and communications

> **States parties should disseminate information and conduct awareness-raising campaigns on the rights of the child in the digital environment, focusing in particular on those whose actions have a direct or indirect impact on children. They should facilitate educational programmes for children, parents and caregivers, the general public and policy makers to enhance their knowledge of children's rights in relation to the opportunities and risks associated with digital products and services. Such programmes should include information on how children can benefit from digital products and services and develop their digital literacy and skills, how to protect children's privacy and prevent victimization, and how to recognise a child who is a victim of harm perpetrated online or offline and respond appropriately. Such programmes should be informed by research and consultations with children, parents and caregivers.**
>
> Source: General comment No. 25 (2021), para 32[257]

Objective:

To raise awareness of all child online safety issues across all sectors of the community, in order to prevent likely harms and promote positive internet use. This information will be disseminated widely, with specific programmes for different audiences.

Model policy text:

To ensure a holistic approach to child online safety, each of the steps below is necessary.

8a. Generate a public awareness programme
Awareness-raising strategies will help people understand and navigate the issue of child online safety while still benefiting from the online space. Materials to be produced should make clear the principles of child online safety and actions that can be taken to understand risk, mitigate harms, report offences and seek redress. This information will be provided in simple terms on official websites. Targeted messages and materials should be designed in consultation with children, young people and parents/carers. It should consider the specific needs of parents/carers and children, with particular attention given to the youngest and most vulnerable children – including those with learning disabilities or those without parental guidance. Peer-to-peer education is a valuable strategy for children of all ages to get to know their rights and responsibilities online. This programme of public messaging can help children and adults to understand the issues and make wise choices about their online interactions, but is not a replacement for formal education, professional training, safety by design or corporate responsibility. Such information should cover the full range of child online safety issues as set out in this policy.

[257] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

The five cross-cutting themes

1. Identifying risk and mitigating harm
2. Promoting access, accessibility and inclusion
3. Building a chain of responsibility and collaboration
4. Integrating child-centred design
5. Ensuring effectiveness

The ten policy action areas

1. Institutional capacity
2. Legal and regulatory frameworks
3. Personal data, identity and autonomy
4. Response and support systems
5. Corporate responsibility
6. Training
7. Education
8. Public awareness and communications
9. Research and development
10. Global cooperation

8b. Provide accessible information and educational materials

Online safety education will start in early childhood and develop according to children's changing needs as they grow: specific materials will be produced to guide and support children of all ages, their families and caregivers. Information materials will promote the positive use of digital technology, sexuality and consent, and will consider the needs of all children, regardless of gender, age, income or background. Information provided by third parties will reflect children's rights and principles and aim to help children of all ages to get to know risks and their rights online. Materials should make clear that children and users are not responsible when bad things happen to them. Community groups, youth clubs, families, religious institutions and digital platforms will all be instrumental in driving effective child online safety awareness and informal education at the community level.

8c. Raise awareness of child online safety in the media

Information to support media coverage of child online safety issues in a child-friendly way should be made available. Media and entertainment companies should be made aware of child online safety and be encouraged to support public awareness campaigns where appropriate, in a balanced, responsible and informative manner. The full range of child online safety issues – not just the most dramatic headlines related to this – should be encouraged.

8d. Engage parents/carers and children in discussions about child online safety

Parents/carers and families should be empowered to understand and take action on child online safety in their own homes. Consultations with families and children are needed to identify issues, solutions and ways of raising awareness of child online safety in an effective way in the community.

< PREVIOUS SECTION NEXT SECTION >

Roadmap to achieving the policy:

A Generate a public awareness programme

Awareness-raising strategies will help people understand and navigate the issue of child online safety while still benefiting from the online space. Materials to be produced should make clear the principles of child online safety and actions that can be taken to understand risk, mitigate harms, report offences and seek redress. This information will be provided in simple terms on official websites.

Targeted messages and materials should be designed in consultation with children, young people and parents/carers, and will consider the specific needs of parents/caregivers and children, with particular attention given to the youngest and most vulnerable children – including those with learning disabilities or those without parental guidance. Peer-to-peer education is a valuable strategy for children of all ages to get to know their rights and responsibilities online. This programme of public messaging can help children and adults to understand the issues and make wise choices about their online interactions, but is not a replacement for formal education, professional training, safety by design or corporate responsibility. Such information should cover the full range of child online safety issues as set out in this policy.

If yes, provide details:

If no, it will help to:

1. Identify key audiences and consult them on what their perceptions and questions are.
2. Identify essential messages that you wish to impart to each audience. See Supportive tool 1.
3. Consider how the message can encourage safe digital use, rather than simply shocking or creating anxiety.
4. Ensure the messaging is not discriminatory, for example, by making it seem that girls should not be online or that online friendships with people of different backgrounds are dangerous.
5. Work with children and parents/carers to develop and/or test your messaging.
6. Consider examples of how different audiences require different messaging.[258]

[258] See for example Rwanda Child Online Protection Policy, 5Rights Foundation, 2019.

< PREVIOUS SECTION

NEXT SECTION >

B Provide accessible information and educational materials

Online safety education will start in early childhood and develop according to children's changing needs as they grow: specific materials will be produced to guide and support children of all ages, their families and caregivers. Information materials will promote the positive use of digital technology, and will consider the needs of all children, regardless of gender, age, income or background. Information provided by third parties will reflect children's rights and principles and aim to help children of all ages to get to know their rights online. Materials should make clear that children and users are not responsible when bad things happen to them. Community groups, youth clubs, families, religious institutions and digital platforms will all be instrumental in driving effective child online safety awareness and informal education at the community level.

If yes, provide details:

If no, it will help to:

1. Identify key audiences.
2. Identify the essential messages that you wish to impart to each audience.
3. Consider how the message can encourage safe digital use, rather than simply shocking or creating anxiety.
4. Ensure the messaging is not discriminatory, for example, by making it seem that girls should not be online or that online friendships with people of different backgrounds are dangerous.
5. Check the examples of different audiences and messaging.

< PREVIOUS SECTION NEXT SECTION >

C Raise awareness of child online safety in the media

Information to support media coverage of child online safety issues in a child-friendly way should be made available. Media and entertainment companies should be made aware of child online safety and be encouraged to support public awareness campaigns where appropriate, in a balanced, responsible and informative manner. The full range of child online safety issues – not just the most dramatic headlines related to this – should be encouraged.

If yes, provide details:

If no, it will help to:

1. Ensure the lead ministry and steering committee develop key messages and KPIs based on the Child Online Safety Toolkit.
2. Build awareness and understanding of the media and develop understanding and sensitivity to language. Where resources allow, undertake media training.
3. Ensure these messages are shared with both mainstream and specialist media, to encourage buy in from the public and to ensure transparency of the roadmap, including its successes and any delays or complications.
4. Make sure key stakeholders and political leaders are available to promote and engage with the full scope of the child online safety roadmap.[259]

[259] Rwanda Child Online Protection Policy, 5Rights Foundation, 2019.

< PREVIOUS SECTION NEXT SECTION >

8 Public awareness and communications

D **Engage parents/carers and children in discussions about child online safety**

Parents/carers and families should be empowered to understand and take action on child online safety in their own homes. Consultations with families and children are needed to identify issues and ways of raising awareness of child online safety in an effective way in the community.

If yes, provide details:

If no, it will help to:

1. Identify government departments, NGOs and professionals that work with or speak directly to children, families and caregivers.
2. Provide opportunities for them to engage with the roadmap and understand the full scope and possibilities it affords.
3. Capture the voices of children, parents/carers in information or policy materials.
4. Provide key messages directed to families and caregivers that speak to their anxieties but also extend their knowledge to a broader understanding of the digital sphere; capture the voices of children speaking directly to parents/carers.[260]

[260] Our Rights in a Digital World, 5Rights Foundation, 2021.

< PREVIOUS SECTION NEXT SECTION >

How this aligns with foundational documents:

> **The range of targets for cyber attacks is increasing quickly. New internetusers typically have low awareness of digital hygiene. Already over half of attacks are directed at 'things' on the Internet of Things, which connects everything from smart TVs to baby monitors to thermostats. Fast 5G networks will further integrate the internet with physical infrastructure, likely creating new vulnerabilities.**
>
> Source: The Age of Digital Interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation 2019[261]

> **States parties should ensure that digital literacy is taught in schools, as part of basic education curricula, from the preschool level and throughout all school years, and that such pedagogies are assessed on the basis of their results. Curricula should include the knowledge and skills to safely handle a wide range of digital tools and resources, including those relating to content, creation, collaboration, participation, socialization and civic engagement. Curricula should also include critical understanding, guidance on how to find trusted sources of information and to identify misinformation and other forms of biased or false content, including on sexual and reproductive health issues, human rights, including the rights of the child in the digital environment, and available forms of support and remedy. They should promote awareness among children of the possible adverse consequences of exposure to risks relating to content, contact, conduct and contract, including cyberaggression, trafficking, sexual exploitation and abuse and other forms of violence, as well as coping strategies to reduce harm and strategies to protect their personal data and those of others and to build children's social and emotional skills and resilience.**
>
> Source: General comment No. 25 (2021), para 104[262]

[261] The Age of Digital Interdependence, UN Secretary-General's High-level Panel on Digital Cooperation, 2019.

[262] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

Supportive tools:

1. Checklist to ensure awareness programme is comprehensive

Process A ('Generate a public awareness programme') requires the development of a general awareness programme that is able to target some very specific audiences. This tool is designed to help you ensure these requirements are met.

Group/audience	Core message to reach them
Younger children under 12	✎
Children 12-18	
Vulnerable children: - In care - With additional needs - With language barriers - Involved in criminal justice settings - Those outside the mainstream education system	
Families with accessibility issues	
Rural and remote families	

< PREVIOUS SECTION

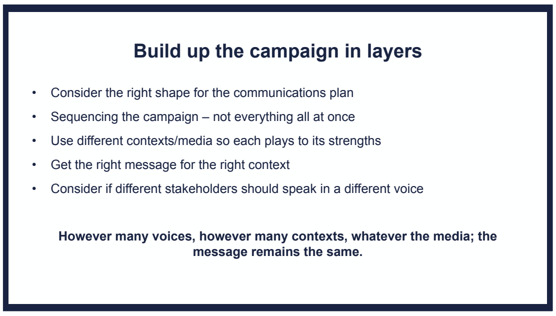
NEXT SECTION >

Other resources for reference:

1. **Child Online Protection in Rwanda – Child Online Protection Communications**[263]
Working on behalf of the Government of Rwanda, 5Rights Foundation prepared some communication materials as part of the implementation of their child online safety policy.

KARMARAMA
GOOD WORKS

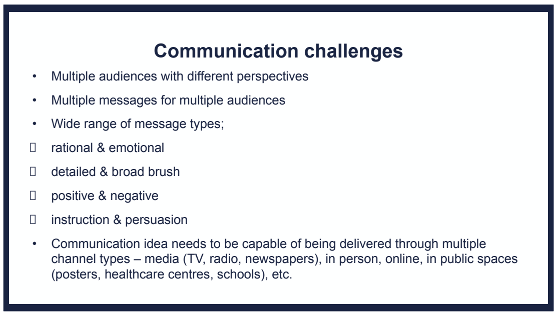
Child Online Protection: Rwanda



Build up the campaign in layers

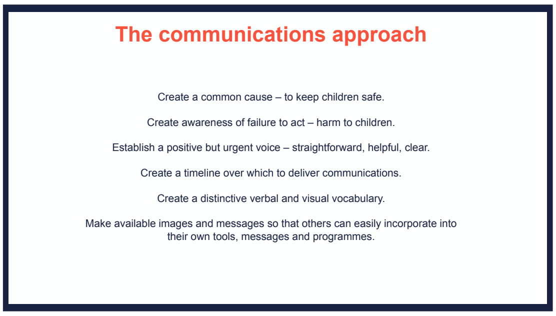
- Consider the right shape for the communications plan
- Sequencing the campaign – not everything all at once
- Use different contexts/media so each plays to its strengths
- Get the right message for the right context
- Consider if different stakeholders should speak in a different voice

However many voices, however many contexts, whatever the media; the message remains the same.



Communication challenges

- Multiple audiences with different perspectives
- Multiple messages for multiple audiences
- Wide range of message types;
 rational & emotional
 detailed & broad brush
 positive & negative
 instruction & persuasion
- Communication idea needs to be capable of being delivered through multiple channel types – media (TV, radio, newspapers), in person, online, in public spaces (posters, healthcare centres, schools), etc.



The communications approach

Create a common cause – to keep children safe.

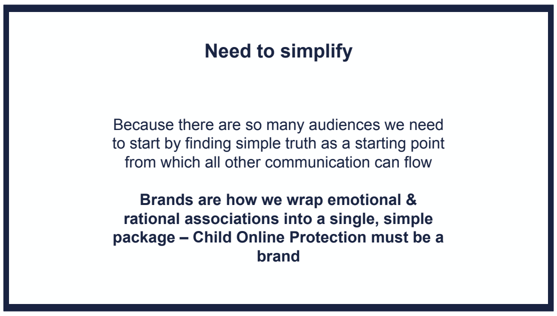
Create awareness of failure to act – harm to children.

Establish a positive but urgent voice – straightforward, helpful, clear.

Create a timeline over which to deliver communications.

Create a distinctive verbal and visual vocabulary.

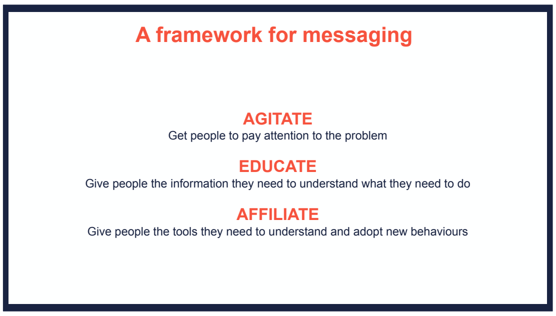
Make available images and messages so that others can easily incorporate into their own tools, messages and programmes.



Need to simplify

Because there are so many audiences we need to start by finding simple truth as a starting point from which all other communication can flow

Brands are how we wrap emotional & rational associations into a single, simple package – Child Online Protection must be a brand



A framework for messaging

AGITATE
Get people to pay attention to the problem

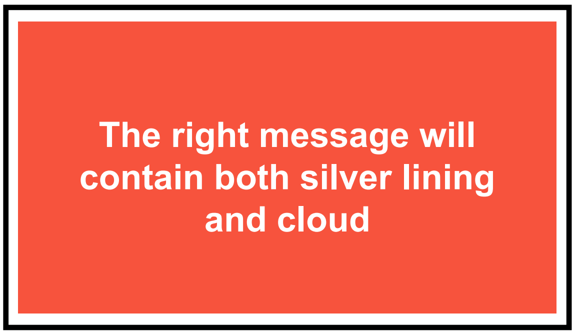
EDUCATE
Give people the information they need to understand what they need to do

AFFILIATE
Give people the tools they need to understand and adopt new behaviours

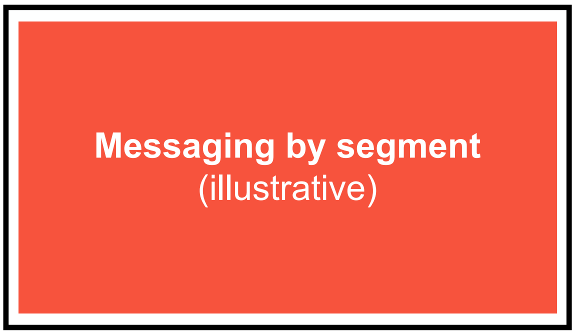
[263] Child Online Protection in Rwanda, 5Rights Foundation, 2019.

< PREVIOUS SECTION NEXT SECTION >

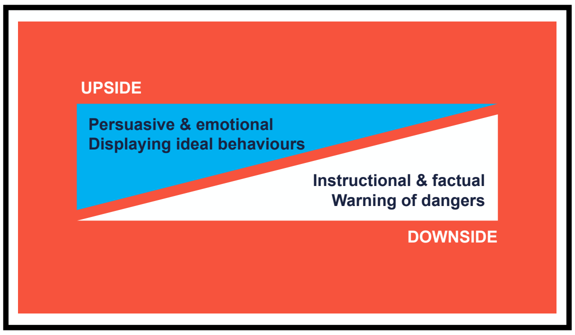
8 Public awareness and communication



The right message will contain both silver lining and cloud



Messaging by segment
(illustrative)

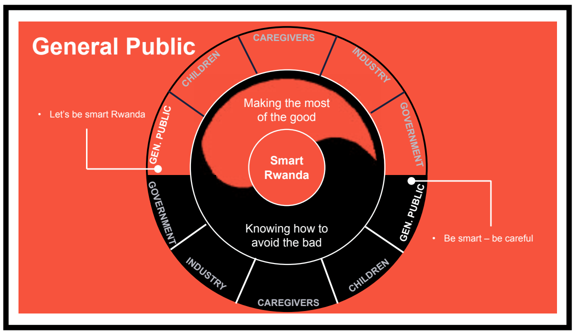


UPSIDE

Persuasive & emotional
Displaying ideal behaviours

Instructional & factual
Warning of dangers

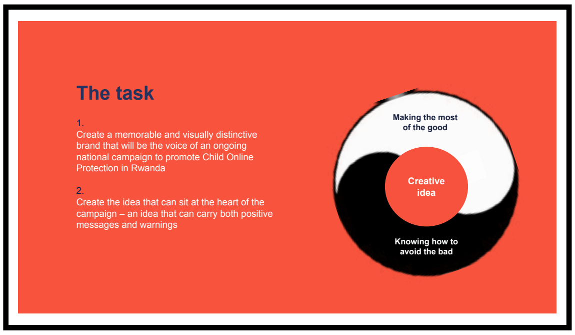
DOWNSIDE



General Public

- Let's be smart Rwanda

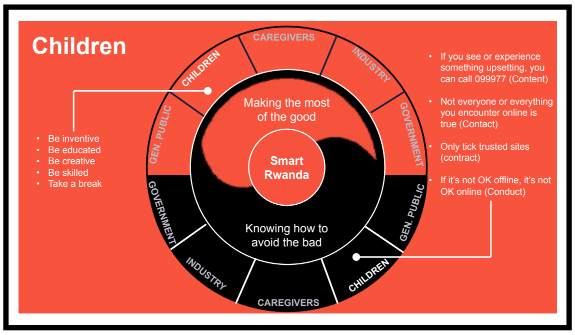
- Be smart – be careful



The task

1.
Create a memorable and visually distinctive brand that will be the voice of an ongoing national campaign to promote Child Online Protection in Rwanda

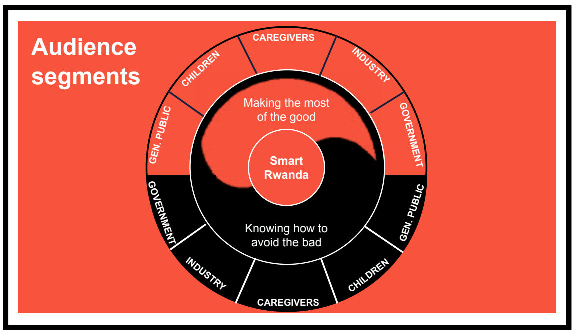
2.
Create the idea that can sit at the heart of the campaign – an idea that can carry both positive messages and warnings



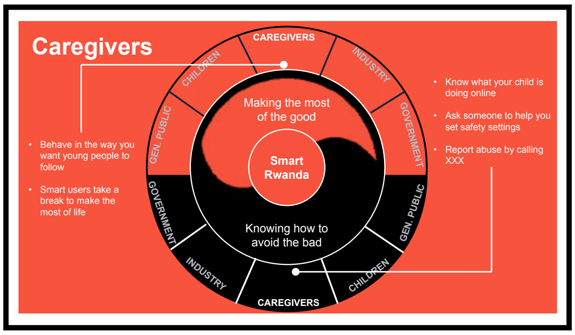
Children

- Be inventive
- Be educated
- Be creative
- Be skilled
- Take a break

- If you see or experience something upsetting, you can call 099977 (Content)
- Not everyone or everything you encounter online is true (Contact)
- Only tick trusted sites (contract)
- If it's not OK offline, it's not OK online (Conduct)



Audience segments



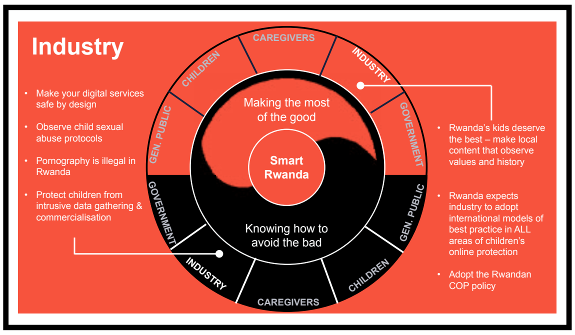
Caregivers

- Behave in the way you want young people to follow
- Smart users take a break to make the most of life

- Know what your child is doing online
- Ask someone to help you set safety settings
- Report abuse by calling XXX

< PREVIOUS SECTION NEXT SECTION >

8 Public awareness and communications

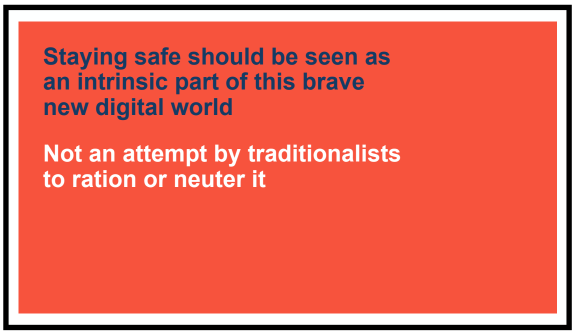


Industry

- Make your digital services safe by design
- Observe child sexual abuse protocols
- Pornography is illegal in Rwanda
- Protect children from intrusive data gathering & commercialisation

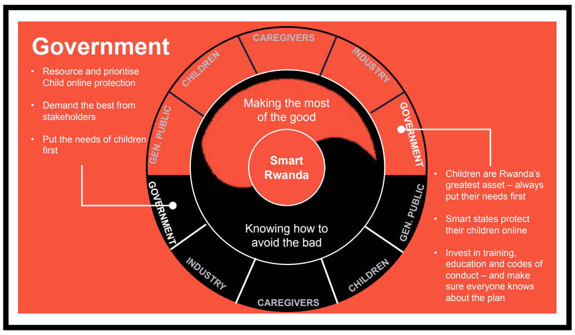
- Rwanda's kids deserve the best – make local content that observe values and history
- Rwanda expects industry to adopt international models of best practice in ALL areas of children's online protection
- Adopt the Rwandan COP policy

CAREGIVERS
INDUSTRY
GOVERNMENT
GEN. PUBLIC
CHILDREN
Making the most of the good
Smart Rwanda
Knowing how to avoid the bad
GEN. PUBLIC
CHILDREN
CAREGIVERS
INDUSTRY
GOVERNMENT



Staying safe should be seen as an intrinsic part of this brave new digital world

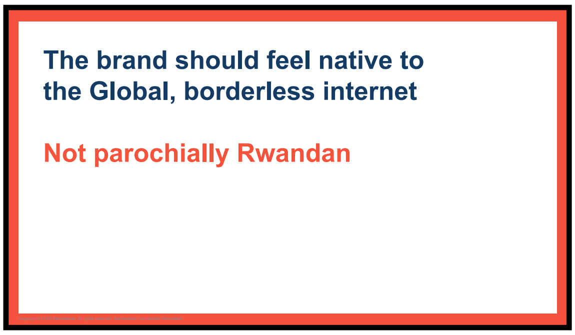
Not an attempt by traditionalists to ration or neuter it



Government

- Resource and prioritise Child online protection
- Demand the best from stakeholders
- Put the needs of children first

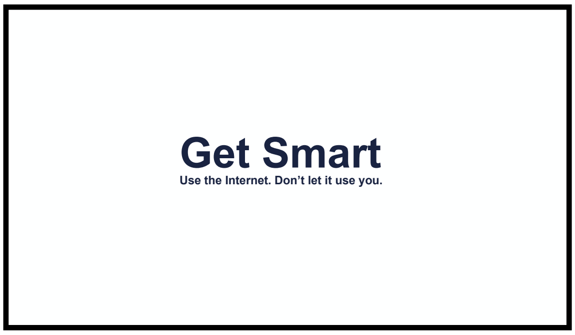
- Children are Rwanda's greatest asset – always put their needs first
- Smart states protect their children online
- Invest in training, education and codes of conduct – and make sure everyone knows about the plan



The brand should feel native to the Global, borderless internet

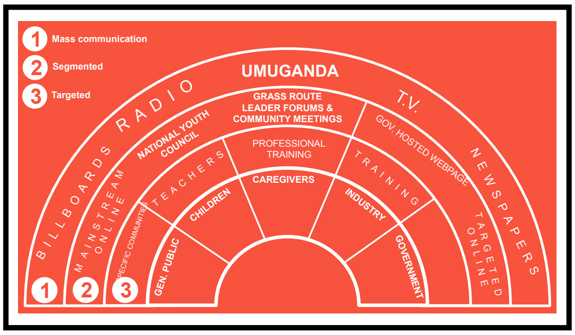
Not parochially Rwandan

Bringing the message to life in all the right places

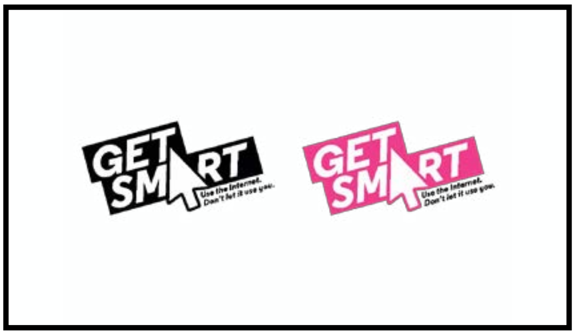


Get Smart

Use the Internet. Don't let it use you.



1 Mass communication
2 Segmented
3 Targeted



GET SMART
Use the Internet. Don't let it use you.
GET SMART
Use the Internet. Don't let it use you.

< PREVIOUS SECTION
NEXT SECTION >

Watching a video online. Simple.
Reporting an offensive video. Smart.

Seen something upsetting? Call xxx to
report it
or find out more at getsmart.rw

2. **5Rights Foundation Twisted Toys campaign**[264]
   This campaign, launched by 5Rights Foundation, raised awareness of any type of surveillance and danger children might face when they are exploring the digital world.

3. **UNESCO Global Media and Information Literacy Week**[265]
   Global Media and Information Literacy Week is an annual event to review the progress of media and information literacy for the public.

4. **Australian eSafety Commissioner's Global Tools for Parents**[266]
   This document, prepared by the Australian eSafety Commissioner's Office, provides guidance for caregivers and parents to help protect children online.

5. **The Council of Europe Digital Parenting Handbook**[267]
   This handbook, prepared by the Council of Europe, provides guidance for caregivers and parents to ensure children's online safety, and especially to protect them from sexual exploitation and abuse.

6. **Goals of Africa Safer Internet Day 2021 with Sango the Mascot**[268]
   With the vision of creating a world where children can be connected and can fully benefit from the opportunities of a trusted and safe online environment, the ITU has outlined the following goals for Africa:

   □ To promote Africa-wide education and awareness on the importance of child online safety.

   □ To raise awareness with governments, industry, educators, children and parents to ensure that the African Child is safe and secure while online.

   □ To design strategies to empower and support the African Child's resilience building.

   □ To develop, share or contextualise available resources to support children's learning and education.

[264] Twisted Toys, 5Rights Foundation, 2021.

[265] Global Media and Information Literacy Week, The United Nations Educational, Scientific and Cultural Organization, 2021.

[266] Global Online Safety Advice for Parents and Carers, eSafety Commissioner, 2020.

[267] Parenting in the Digital Age, Council of Europe, 2017.

[268] Positioning and Partnering for Child Online Protection, International Telecommunication Union (ITU) Regional Office for Africa, 2021.

< PREVIOUS SECTION NEXT SECTION >

7. **Case Study: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia**[269]
The Colombian Ministry of Information Technologies and Communications promotes the development of digital skills to confidently face the risks associated with the use of the internet and ICT.

Target audience:

🟩 6 to 18 year olds

🟩 Academia 11 to 28 years old

🟩 Adults age 28 years plus

It has a website that provides links to FAQs, training and educational resources and accessible information on the digital world.

8. **e-Learning course: Action to End Child Sexual Exploitation and Abuse**[270]
Action to End Child Sexual Exploitation and Abuse is an e-learning course designed to increase awareness and knowledge about child sexual exploitation and abuse, including abuse facilitated by technology, and promote evidence-based strategies and actions for prevention and response. The course covers policy, advocacy and a wide range of programmatic aspects. The review and e-learning course have been produced with financial support from the End Violence Fund.

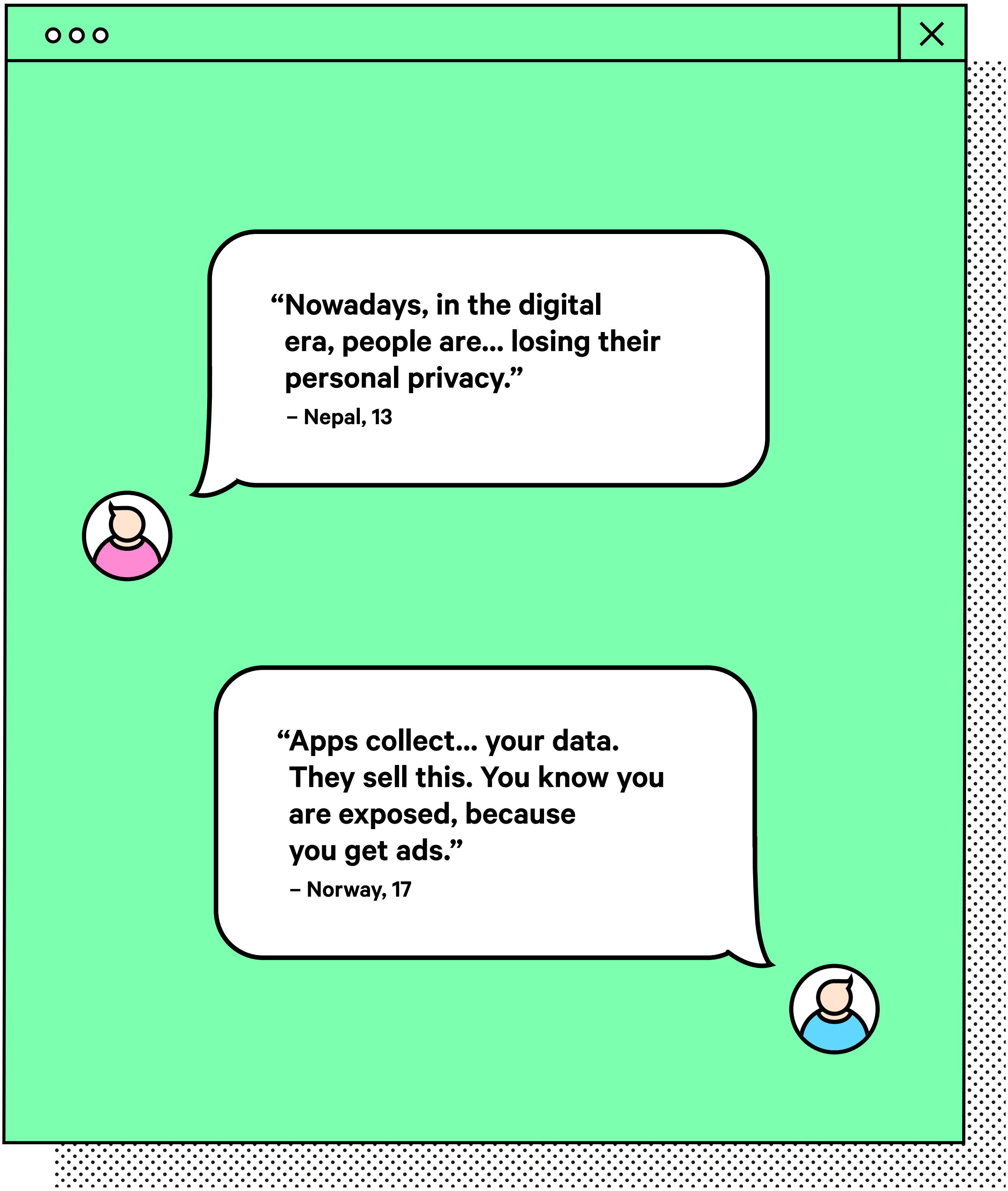
9. **WeProtect Global Alliance How to talk about child sexual abuse in the digital world**[271]
This strategic brief outlines challenges for communicating about child sexual exploitation and abuse online. And offers preliminary recommendations for communicators.

[269] En TIC confío+, Ministry of Information Technologies and Communications of Colombia, 2021.

[270] Action to End Child Sexual Exploitation and Abuse, UNICEF, 2022.

[271] How to talk about child sexual abuse in the digital world, WeProtect Global Alliance, 2021.

< PREVIOUS SECTION NEXT SECTION >



"Nowadays, in the digital era, people are... losing their personal privacy."

– Nepal, 13

"Apps collect... your data. They sell this. You know you are exposed, because you get ads."

– Norway, 17

< PREVIOUS SECTION NEXT SECTION >

9 Research and development

> **Regularly updated data and research are crucial to understanding the implications of the digital environment for children's lives, evaluating its impact on their rights and assessing the effectiveness of State interventions. States parties should ensure the collection of robust, comprehensive data that is adequately resourced and that data are disaggregated by age, sex, disability, geographical location, ethnic and national origin and socioeconomic background. Such data and research, including research conducted with and by children, should inform legislation, policy and practice and should be available in the public domain. Data collection and research relating to children's digital lives must respect their privacy and meet the highest ethical standards.**
>
> Source: General comment No. 25 (2021), para 30[272]

Objective:

To ensure a holistic and up to date approach to child online safety, each of the steps below is necessary.

Model policy text:

To establish and fund effective and publicly accessible national and regional child online safety research and development frameworks to support child online safety policy development and implementation.

9a. Establish child online safety research frameworks
Countries should establish a central research fund to develop a research programme with clearly identified terms of reference and objectives that remain current, in order to enable ongoing research in child online safety across a broad range of relevant issues. Where possible, countries should reach out and cooperate with each other on child online safety research and development. Gap analysis should help to ensure resources are prioritised in areas of biggest need and to avoid unnecessary duplication. Research should be made available to regional or international partners, particularly those with the least resource.

9b. Continued innovation
Research evidence will inform the development of products and services that incorporate safety by design; enable the evaluation of child online safety practice; and provide an understanding of children's online experiences and solutions in the national context.

9c. Establish centres of excellence in research and development in child online safety
Countries should develop centres of excellence within existing institutions (universities, health settings, innovation hubs) that can share and cooperate on the development of tools, services and skills relating to child online safety through national, regional and international engagement. ▶

[272] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION NEXT SECTION >

9d. Establish strong ethical frameworks for research and development in child online safety[273]
Countries should develop guidelines for researchers working on child online safety, including effective consideration of children's rights as part of the research process. This should include clear guidance on data collection and the ethics and rights implications of processing children's data. The interests of the child should be the primary consideration within ethical frameworks for research and development on child online safety, including in situations of public interest access.

9e. Establish frameworks for information gathering
Regulators working in child online safety should set up frameworks for information gathering that will allow them to monitor and evaluate the effectiveness of child online safety in different contexts and the impact it has on different groups of children. Monitoring and evaluation of child online safety actions should form part of the research and development process.

9f. Enable access to private companies' data in the public interest
Frameworks should be created where social media and other companies must share their data to support research in the best interests of the child.

9g. Ensure that data and statistics are relevant to the context
Statistical models should reflect the local picture, to support the level of understanding and response to national issues. They should allow for monitoring of cross-border impacts.

[273] Children and the Data Cycle: Rights and Ethics in a Big Data World, United Nations Children's Fund, 2017.

< PREVIOUS SECTION NEXT SECTION >

9 Research and development

Roadmap to achieving the policy:

A Establish child online safety research frameworks

Countries should establish a central research fund to develop a research programme with clearly identified terms of reference and objectives that remain current, in order to enable ongoing research in child online safety across a broad range of relevant issues. Where possible, countries should reach out and cooperate with each other on child online safety research and development. Gap analysis should help to ensure resources are prioritised in areas of biggest need and to avoid unnecessary duplication. Research should be made available to regional or international partners, particularly those with the least resource.

If yes, provide details:

If no, it will help to:

1. Identify existing research funds and/or institutions that might house or fund research into child online safety.
2. Identify the area of research that is required.
3. Establish strict criteria for ensuring that the research contributes to the literacy, safety and wellbeing of children.
4. Ensure that those undertaking research are aware of all the areas of the policy roadmap and do not concentrate solely on one area.
5. Make all funding of research dependent on the wide sharing of outcomes, including holding research findings in a central repository and making funds available for dissemination and policy uptake.

< PREVIOUS SECTION NEXT SECTION >

B **Continued innovation**

Research evidence will inform the development of products and services that incorporate safety by design; enable the evaluation of child online safety practice; and provide an understanding of children's online experiences in the national context.

If yes, provide details:

If no, it will help to:

1. Map changes – globally – to products and services and share widely, to ensure advances made in child safety in one part of the world are available to other parts of the world.
2. Map where advances have been made, and involve international NGOs or expert groups in supporting their dissemination.
3. Leverage arrangements with intergovernmental organisations, private companies and NGOs to spread good practice – for example, a donation of computer hardware should be conditional on incorporating safety and privacy features by default.

C **Establish centres of excellence in research and development in child online safety**[274]

Countries should develop child online safety hubs that can share and cooperate on the development of tools, services and skills relating to child online safety through national, regional and international engagement.

If yes, provide details:

If no, it will help to:

1. House child online safety hubs in existing government departments or academic institutions.
2. Consider setting up child online safety hubs across regions with similar cultural and organisational requirements, to share best practice.

[274] Child Safety Online Global Challenges and Strategies, United Nations Children's Fund, 2011.

< PREVIOUS SECTION

NEXT SECTION >

D Establish strong ethical frameworks for research and development in child online safety[275]

Countries should develop guidelines for researchers working on child online safety, including effective consideration of children's rights as part of the research process. This should include clear guidance on data collection and the ethics and rights implications of processing children's data. The interests of the child should be the primary consideration within ethical frameworks for research and development on child online safety, including in situations of public interest access.

If yes, provide details:

If no, it will help to:

1. Establish minimum standards of responsible research (see Resources below, e.g. ECPAT Guidelines).
2. Ensure that the standards are built into the funding and/or acceptance of research results. See Supportive tools 1 (page no. 156).
3. Ensure child safety training for researchers is mandatory (see Policy action area on Training, page no. 144).

E Establish frameworks for information gathering

Regulators working in child online safety should set up frameworks for information gathering that will allow them to monitor and evaluate the effectiveness of child online safety in different contexts and the impact it has on different groups of children. Monitoring and evaluation of child online safety actions should form part of the research and development process.

If yes, provide details:

If no, it will help to ensure regulators require information gathering frameworks to understand inputs, methods and outcomes. Any legal or regulatory requirements should include reporting, transparency and information gathering powers. Examples are the GDPR[276] and the UK's draft Online Safety Bill.[277]

[275] Children and the Data Cycle: Rights and Ethics in a Big Data World, United Nations Children's Fund, 2017.

[276] General Data Protection Regulation, European Union, 2018.

[277] Draft Online Safety Bill, Department for Digital, Culture, Media, 2021.

< PREVIOUS SECTION

NEXT SECTION >

F Enable access to private companies' data in the public interest

Frameworks should be created where social media and other companies must share their data to support research in the best interests of the child.

If yes, provide details:

If no, it will help to:

1. Conduct outreach to social media companies in the relevant territory, requesting access to data sets where appropriate.
2. Join in regional, national or global conversations making similar requests.

G Ensure that data and statistics are relevant to the context

Regulators working in child online safety should set up frameworks for information gathering that will allow them to monitor and evaluate the effectiveness of child online safety in different contexts and the impact it has on different groups of children. Monitoring and evaluation of child online safety actions should form part of the research and development process.

If yes, provide details:

If no, it will help to:

1. Source and find statistics that are from well-documented and reputable agencies.
2. Engage with stakeholders from these agencies to validate and confirm your statistics.

< PREVIOUS SECTION NEXT SECTION >

How this aligns with foundational documents:

> **Capability 2 Model National Response – Research, analysis and monitoring of law enforcement good practice:**
>
> **At a minimum, an analysis should: assess the current CSEA threat, how it is manifested and who is most at risk; assess the country's vulnerability to this threat; assess the current institutional response; review and evaluate the implementation of applicable legislation and policies to assess compliance with international standards and good practice; review the current ICT ecosystem response – including Hotline reporting mechanisms and industry engagement; and map the activity of other stakeholders engaged in this issue.**
>
> **To inform an analysis, access needs to be provided to a wide range of CSEA relevant data and information from organisations represented on the national body and any other relevant stakeholders. In addition, primary data needs to be collected from a variety of sources such as children, parents, educators, law enforcers, service providers.**
>
> Source: WeProtect Global Alliance Model National Response (MNR), pages 5-6[278]

[278] Model National Response, WeProtect Global Alliance, 2016.

< PREVIOUS SECTION NEXT SECTION >

Supportive tools:

1. Checklist of research ethics considerations

Process D ('Establish strong ethical frameworks for research and development in child online safety') outlines the need to think holistically about research ethics in methodology, funding and data collection. This checklist is designed to help ensure your research ethics frameworks address these areas.

Does selection of research for government funding take account of child online safety?

If yes, provide details:

If no, how will this be addressed?

Does funding for research include a child impact assessment or ethical review?

If yes, provide details:

If no, how will this be addressed?

< PREVIOUS SECTION NEXT SECTION >

9 Research and development

Is there an ethical framework for researchers and developers including children's rights perspectives?

If yes, provide details:

If no, how will this be addressed?

Are researchers, developers and funding decision makers trained on child online safety and children's rights?

If yes, provide details:

If no, how will this be addressed?

< PREVIOUS SECTION

NEXT SECTION >

9 Research and development

Is the precautionary principle applied to research and development?

If yes, provide details:

If no, how will this be addressed?

Is open-source data available to support child online safety research?

If yes, provide details:

If no, how will this be addressed?

< PREVIOUS SECTION NEXT SECTION >

Other resources for reference:

1. **University of Oxford – Framework for Responsible Research and Innovation in ICT**[279]
Funded by the Engineering and Physical Sciences Research Council (EPSRC), this framework explores ethical issues in ICT research. Prepared by the Observatory for Responsible Research and Innovation in ICT (ORBIT), it provides clear instructions on how to conduct practical and ethical research.

2. **End Violence Partnership – Disrupting Harm**[280]
In partnership with EPCAT International, INTERPOL and the UNICEF Office of Research, with funding from the End Violence Partnership, Disrupting Harm is a research project that unpacks how digital technology facilitates the sexual exploitation and abuse of children across 13 countries in Eastern and Southern Africa and Southeast Asia.

3. **ECPAT Guidelines for Ethical Research on the Sexual Exploitation of Children**[281]
This is a guide for researchers looking to conduct research on issues relating to the sexual exploitation and abuse of children, which raises certain ethical issues and dilemmas. These guidelines help researchers to shape their research project in ways that minimise harm to children.

4. **EU Fundamental Rights Agency Opinion**[282]
Fundamental Rights Agency Opinion 9: Whenever they fund research and development activities, the EU and its Member States should require contractors to involve experts on personal data protection and other fundamental rights. Scientific researchers and industry should pay attention to the effect of phenotypical characteristics, as well as age and gender, on the composition of test groups, to eliminate any risks of discriminatory outcomes of test results.

5. **UN Office of the High Commissioner for Human Rights – Guidance on a Human Rights Based Approach to Data**[283]
This guidance provides recommendations and principles for data stakeholders and policy makers to improve their use of data and statistics. It ensures respect, protection and fulfilment of human rights based on the 2030 Agenda being adopted when collecting or disaggregating data.

[279] A Framework for Responsible Research and Innovation in ICT, University of Oxford, 2014.

[280] Disrupting Harm, End Violence Partnership, 2019.

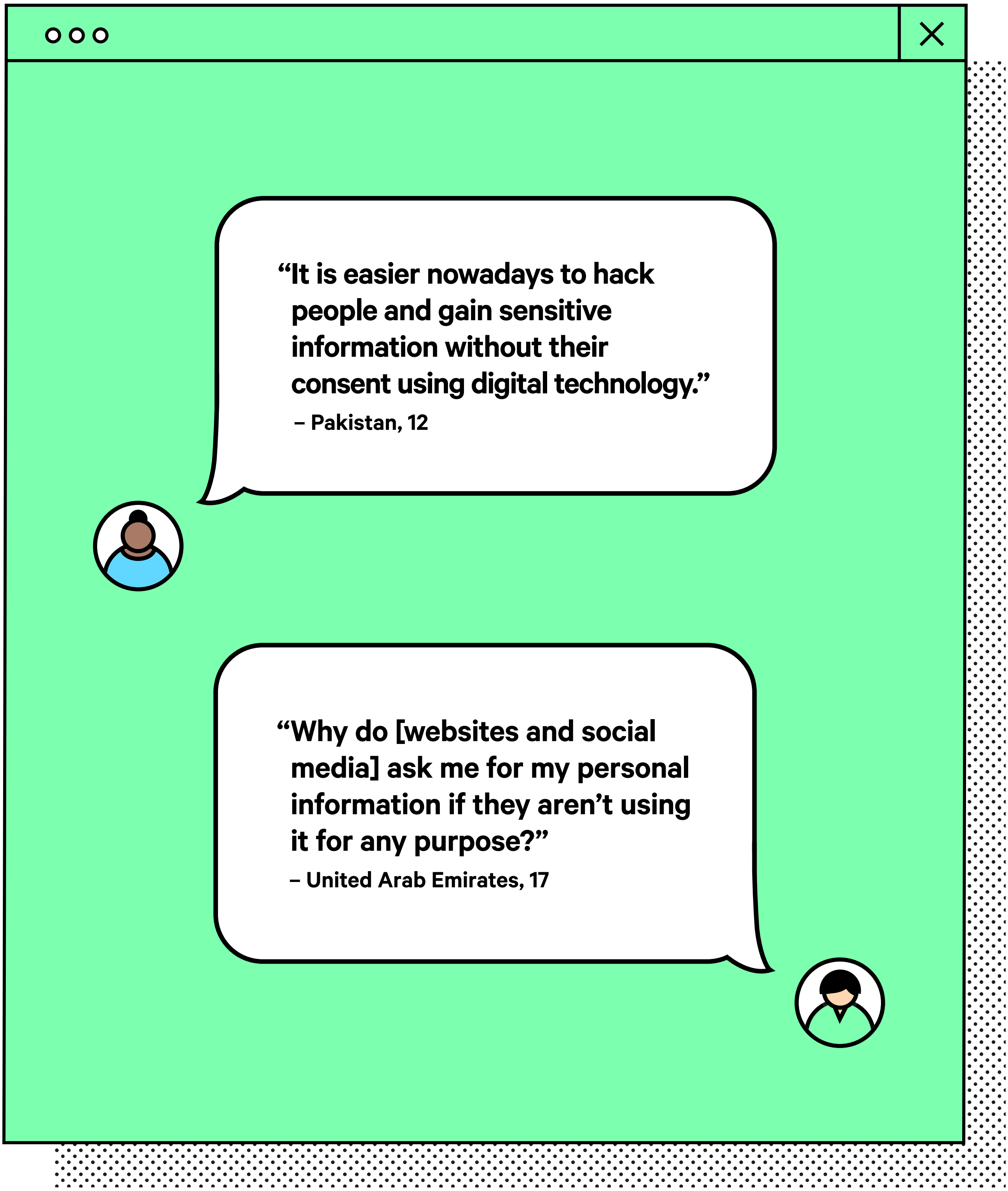
[281] Guidelines for ethical research on sexual exploitation involving children, ECPAT International, 2019.

[282] Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights, European Union Agency for Fundamental Rights, 2018.

[283] A Human Rights-Based Approach to Data, Office of the United Nations High Commissioner for Human Rights, 2018.

< PREVIOUS SECTION

NEXT SECTION >



> “It is easier nowadays to hack people and gain sensitive information without their consent using digital technology.”
>
> – Pakistan, 12

> “Why do [websites and social media] ask me for my personal information if they aren’t using it for any purpose?”
>
> – United Arab Emirates, 17

< PREVIOUS SECTION NEXT SECTION >

10 Global cooperation

> **The cross-border and transnational nature of the digital environment necessitates strong international and regional cooperation, to ensure that all stakeholders, including States, businesses and other actors, effectively respect, protect and fulfil children's rights in relation to the digital environment. It is therefore vital that States parties cooperate bilaterally and multilaterally with national and international non-governmental organizations, United Nations agencies, businesses and organizations specialised in child protection and human rights in relation to the digital environment.**
>
> **States parties should promote and contribute to the international and regional exchange of expertise and good practices and establish and promote capacity building, resources, standards, regulations and protections across national borders that enable the realization of children's rights in the digital environment by all States. They should encourage the formulation of a common definition of what constitutes a crime in the digital environment, mutual legal assistance and the joint collection and sharing of evidence.**
>
> Source: General comment No. 25 (2021), paras 123 & 124[284]

Objective:

To collaborate with national, regional, and global organisations and players to share best practice.

Model policy text:

To ensure a holistic approach to child online safety, each of the steps below is necessary.

10a. Establish formal relationship frameworks (e.g. a Memorandum of Understanding [MoU]) with regional and global child online safety communities
Strengthening international cooperation to enhance child online safety across the globe is critical to guarantee global security. Countries should formalise collaborations for joint Public Private Partnership investments in areas related to cybersecurity, child online safety capacity building, innovation, law enforcement, the justice system and education, among others.

10b. Sign up to regional and international legal instruments that promote cooperation on child online safety
Countries should identify key regional and international instruments that will allow them to cooperate with other countries on child online safety. This should include, among other things: international agreements on law enforcement cooperation; international best practice; international programmes that may provide resources for cooperation on child online safety; and access to any human rights or related standards that will facilitate cooperation between countries. ▶

[284] General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

< PREVIOUS SECTION
NEXT SECTION >

10c. Identify partner countries and organisations that can provide appropriate models and support for child online safety development

It may not be necessary to start policy development from scratch. Countries should look for relevant examples of child online safety frameworks and tools that they may use and adapt to their own context. Sharing information on challenges and problems encountered in child online safety can be very valuable for the planning, development and implementation of child online safety policies.

10d. Support other countries developing child online safety policies

Where appropriate, share model laws, regulatory frameworks, lessons learned or other materials that can be used by other countries to develop their own child online safety frameworks and policies.[285]

Roadmap to achieving the policy:

A **Establish formal relationship frameworks (e.g. MoUs) with regional and global child online safety communities**

Strengthening international cooperation to enhance child online safety across the globe is critical to guarantee global security. Countries should formalise collaborations for joint PPP investments in areas related to cybersecurity, child online safety capacity building, innovation, law enforcement, the justice system and education, among others.

If yes, provide details:

If no, it will help to:

1. Identify relevant regional and global child online safety agreements and treaties (see Key Documents).
2. Arrange to sign up and add necessary steps to your child online safety roadmap.
3. Check these include, at a minimum, any actions required as set out by the:

- □ Sustainable Development Goals[286]
- □ Convention on the Rights of the Child, and its Optional Protocols[287]
- □ General comment No. 25 (2021) on children's rights in relation to the digital environment.[288]
- □ Model National Response.[289] See Supportive tool 1 (page no. 166).

[285] See for example the Australian eSafety Commissioner's International Leadership and Collaboration Materials, 2021.

[286] Transforming our world: the 2030 Agenda for Sustainable Development, United Nations, 2021.

[287] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989.

[288] General comment No. 25 (2021) on children's rights in relation to the digital environment, United Nations Committee on the Rights of the Child, 2021.

[289] Model National Response, WeProtect, 2016.

< PREVIOUS SECTION NEXT SECTION >

B Sign up to regional and international legal instruments that promote cooperation on child online safety

Countries should identify key regional and international instruments that will allow them to cooperate with other countries on child online safety. This should include, among other things: international agreements on law enforcement cooperation; international best practice; international programmes that may provide resources for cooperation on child online safety; and access to any human rights or related standards that will facilitate cooperation between countries.

If yes, provide details:

If no, it will help to:

1. Consult with international enforcement agencies, such as INTERPOL[290] and Europol.[291]
2. Seek best practice from global organisations such as the National Center for Missing & Exploited Children[292] and Internet Watch Foundation.[293]

[290] Who we are, INTERPOL.

[291] About Europol, Europol.

[292] Our work, National Center for Missing and Exploited Children (NCMEC).

[293] About us, Internet Watch Foundation (IWF).

< PREVIOUS SECTION NEXT SECTION >

C Identify partner countries and organisations that can provide appropriate models and support for child online safety development

It may not be necessary to start policy development from scratch. Countries should look for relevant examples of child online safety frameworks and tools that they may use and adapt to their own context. Sharing information on challenges and problems encountered in child online safety can be very valuable for the planning, development and implementation of child online safety policies.

If yes, provide details:

If no, it will help to reach out to regional bodies, such as the Child Rights Coalition Asia,[294] country leaders such as the Alana Foundation in Brazil,[295] or expert organisations such as the Internet Watch Foundation,[296] 5Rights Foundation,[297] UNICEF,[298] INHOPE[299] or the Safe Online Initiative at the Global Partnership to End Violence against Children.[300]These organisations will have resources and information, and in many cases can help you to identify local or relevant partners.

[294] About us, Child Rights Coalition Asia.

[295] About us, Alana Foundation.

[296] About us, Internet Watch Foundation (IWF).

[297] 5Rights Foundation, 5Rights Foundation.

[298] About Us, UNICEF.

[299] Our Story, INHOPE, 2021.

[300] Safe Online, End Violence Against Children, 2022.

< PREVIOUS SECTION NEXT SECTION >

D Support other countries developing child online safety policies

Where appropriate, share model laws, regulatory frameworks, lessons learned or other materials that can be used by other countries to develop their own child online safety frameworks and policies.[301]

If yes, provide details:

If no, it will help to:

1. Identify other organisations and/or lead ministries in your region.
2. Consider best practice from other regions, e.g. the Association of Southeast Asian Nations (ASEAN) or the EU.
3. Share your resources and solutions generously.
4. Consider how you might form partnerships with those with less resource.
5. Encourage recipients to share onwards.
6. Harmonise with best international practice and proactively seek to share with or otherwise enable those countries with less resource: for example, twinning with a particular country or region, supplying technical support such as legal or language translation for parts of the roadmap, or providing workshops for frontline workers – including enforcement.

How this aligns with foundational documents:

> **We recommend that, as a matter of urgency, the UN Secretary-General facilitate an agile and open consultation process to develop updated mechanisms for global digital cooperation, with the options discussed in Chapter 4 as a starting point. We suggest an initial goal of marking the UN's 75th anniversary in 2020 with a 'Global Commitment for Digital Cooperation' to enshrine shared values, principles, understandings and objectives for an improved global digital cooperation architecture. As part of this process, we understand that the UN Secretary-General may appoint a Technology Envoy.**
>
> **5B: We support a multi-stakeholder 'systems' approach for cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the fast-hanging digital age.**
>
> Source: The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation 2019[302]

[301] See, for example, Australia's eSafety Commissioner's International Leadership and Collaboration Materials.

[302] The Age of Digital Interdependence, UN Secretary-General's High-level Panel on Digital Cooperation, 2019.

< PREVIOUS SECTION NEXT SECTION >

Supportive tools:

1. Checklist of international frameworks to meet

Process A ('Establish formal relationship frameworks [e.g. MoUs] with regional and global child online safety communities') outlines that minimum requirements in a range of international protocols and best practice documents must be met. Lead ministries should work across government with the help of this tool to assess compliance.

	Describe how minimum requirements are met	**Gaps in compliance**	**Date the lead ministry is notified about these gaps**	**Date the child online safety stakeholder group is notified about these gaps**
UN Sustainable Development Goals	✎			
UN Convention on the Rights of the Child				
CRC Optional Protocol: Involvement of children in armed conflict				
Sale of children, child prostitution and child pornography				
Communications procedure				

< PREVIOUS SECTION NEXT SECTION >

10 Global cooperation

	Describe how minimum requirements are met	Gaps in compliance	Date notified the lead Ministry about these gaps?	Date notified the child online safety Stakeholder Group about these gaps?
General comment No. 25 (2021)	✎			
Model National Response				
Luxembourg Guidelines on Terminology for the Protection of Children from Sexual Exploitation and Abuse				

Other resources for reference:

Frameworks to support international cooperation

1. **UN Roadmap for Digital Cooperation**[303]
   The Secretary-General's Roadmap for Digital Cooperation,[304] supported by a High-level Panel on Digital Cooperation was released in 2020. It provides recommendations to different stakeholders on strengthening global digital cooperation.

2. **INTERPOL's Crimes Against Children web resource**[305]
   INTERPOL's website provides a range of resources, including information about INTERPOL's work, as well as information about the online CSEA database, blocking and categorising content, and victim identification.

3. **OECD Recommendation of the Council on Children in the Digital Environment**[306]
   The Recommendation sets out principles and guidance to help countries find a balance between protecting children from online risks and promoting the opportunities and benefits that the digital world provides.

[303] United Nations Secretary-General's Roadmap for Digital Cooperation, United Nations, 2020.

[304] United Nations Secretary-General's High-level Panel on Digital Cooperation, United Nations, 2020.

[305] Crimes against children, INTERPOL.

[306] Recommendation of the Council on Children in the Digital Environment, OECD, adopted 2012, amended 2021.

< PREVIOUS SECTION NEXT SECTION >

Other resources for reference:

Frameworks to support regional cooperation

1. **African Union Malabo Convention on Cyber Security and Personal Data Protection 2014**[307]
   This is the African Union's convention to create a 'credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, promotion of cybersecurity, e-governance and combating cybercrime.'

2. **African Union Agenda for Children 2040**[308]
   The African Union's agenda for the year 2040, Agenda 2063, outlines goals for children across the continent. The agenda builds on Paragraph 53 which states that 'African children shall be empowered through the full implementation of the African Charter on the Rights of the Child'.

3. **European Commission Better Internet for Kids Strategy**[309]
   This is the European Commission's European strategy for a better internet for children. The strategy addresses digital skills and tools for children and also outlines the potential of the market to develop interactive, creative and educational online content.

4. **WeProtect Global Alliance Model National Response (MNR)**[310]
   The Model National Response (MNR) is focused on helping countries to build their response to online child sexual exploitation and abuse, but it indicates that this cannot be addressed in isolation. A wider set of capabilities to prevent and tackle child sexual exploitation and abuse is required to be in place to ensure a complete national response.

5. **Better Internet for Kids (BIK) Policy Map**[311]
   The Better Internet for Kids (BIK) Policy Map provides a comprehensive overview of BIK strategies and policies that are currently being implemented across EU member states.

6. **ASEAN Regional Plan of Action on the Elimination of Violence Against Children**[312] **and Declaration on the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN**[313]
   The Regional Plan provides a roadmap to assist member states in implementing the 2013 ASEAN declaration on protecting children from all forms of online exploitation. ▶

[307] African Union Convention on Cyber Security and Personal Data Protection, African Union, 2014.

[308] Africa's Agenda for Children 2040 Fostering an Africa Fit for Children, African Committee of Experts on the Rights and Welfare of the Child, 2016.

[309] A European Strategy for a better Internet for our children, European Commission, 2021.

[310] Model National Response, WeProtect Global Alliance, 2016.

[311] Better Internet for Kids Policy Map, Better Internet for Kids, 2020.

[312] ASEAN Regional Plan of Action on Elimination of Violence against Children, United Nations Children's Fund, 2019.

[313] Ending violence against children in ASEAN Member States, UNICEF East Asia & Pacific, 2019.

< PREVIOUS SECTION NEXT SECTION >

7. **Case Study – Council of Europe Conventions**
The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, also known as "the Lanzarote Convention",[314] requires criminalisation of all kinds of sexual offences against children. It sets out that states in Europe and beyond shall adopt specific legislation and take measures to prevent sexual violence, to protect child victims and to prosecute perpetrators.

The "Lanzarote Committee"[315] (i.e. the Committee of the Parties to the Lanzarote Convention) is the body established to monitor[316] whether Parties effectively implement the Lanzarote Convention. The Committee is also charged with identifying good practices,[317] in particular during capacity-building activities[318] (study visits, conferences, etc.).

The Council of Europe helps to protect societies worldwide from the threat of cybercrime through the Budapest Convention on Cybercrime and its Protocol on Xenophobia and Racism, the Cybercrime Convention Committee (T-CY) and the technical cooperation programmes on cybercrime.

The convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

8. **Organization of American States Preliminary Principles and Recommendations on Data Protection (Protection of Personal Data)[319]**
This is the result of an Inter-American Juridical Committee study of data protection frameworks. The Principles represent a model for Inter-American law on access to public information. They represent the General Secretariat's direction for support to member states on the design, execution and evaluation of their local legal frameworks regarding access to public information.

Inter-country cooperation and buddy support frameworks

9. **Luxembourg Guidelines on Terminology for the Protection of Children from Sexual Exploitation and Abuse[320]**
These guidelines are an initiative by 18 international partners to harmonise terms and definitions related to child protection. They aim to provide greater conceptual clarity on terminology in order to ensure stronger and more consistent advocacy, policy and laws in all languages across all regions of the world.

10. **Police Scotland support for development of a Child Online Policy in Rwanda[321]**
This is a partnership between Police Scotland and the Government of Rwanda. 5Rights Foundation has a detailed blog post describing the partnership.

[314] Lanzarote Convention, Council of Europe.
[315] Lanzarote Committee, Council of Europe.
[316] Lanzarote Convention Monitoring, Council of Europe.
[317] Lanzarote Convention Good practices, Council of Europe.
[318] Lanzarote Convention, Council of Europe.
[319] Preliminary Principles and Recommendations on Data Protection, Permanent Council of the Organisation of American States, 2011.
[320] Luxembourg Guidelines, ECPAT, 2016.
[321] Working with the Government of Rwanda and Police Scotland to support children online, 5Rights Foundation, 2020.

< PREVIOUS SECTION NEXT SECTION >

11. **The Child Online Safety Universal Declaration**[322]
    This is the Broadband Commission's Declaration, which aims to align all relevant stakeholders on the common mission of championing the cause of protection of children online.

Examples of cooperation between law enforcement[323]

12. **The Virtual Global Taskforce**[324]
    This task force represents national, regional and international law enforcement agencies that have come together to combat online child sexual abuse worldwide. It also provides links to regional law enforcement and CSAM reporting hotlines.

13. **The Council of Europe's Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime**[325]
    This is a set of guidelines developed to help service providers and law enforcement communities in any country to establish effective working relationships. It is available in more than a dozen languages.

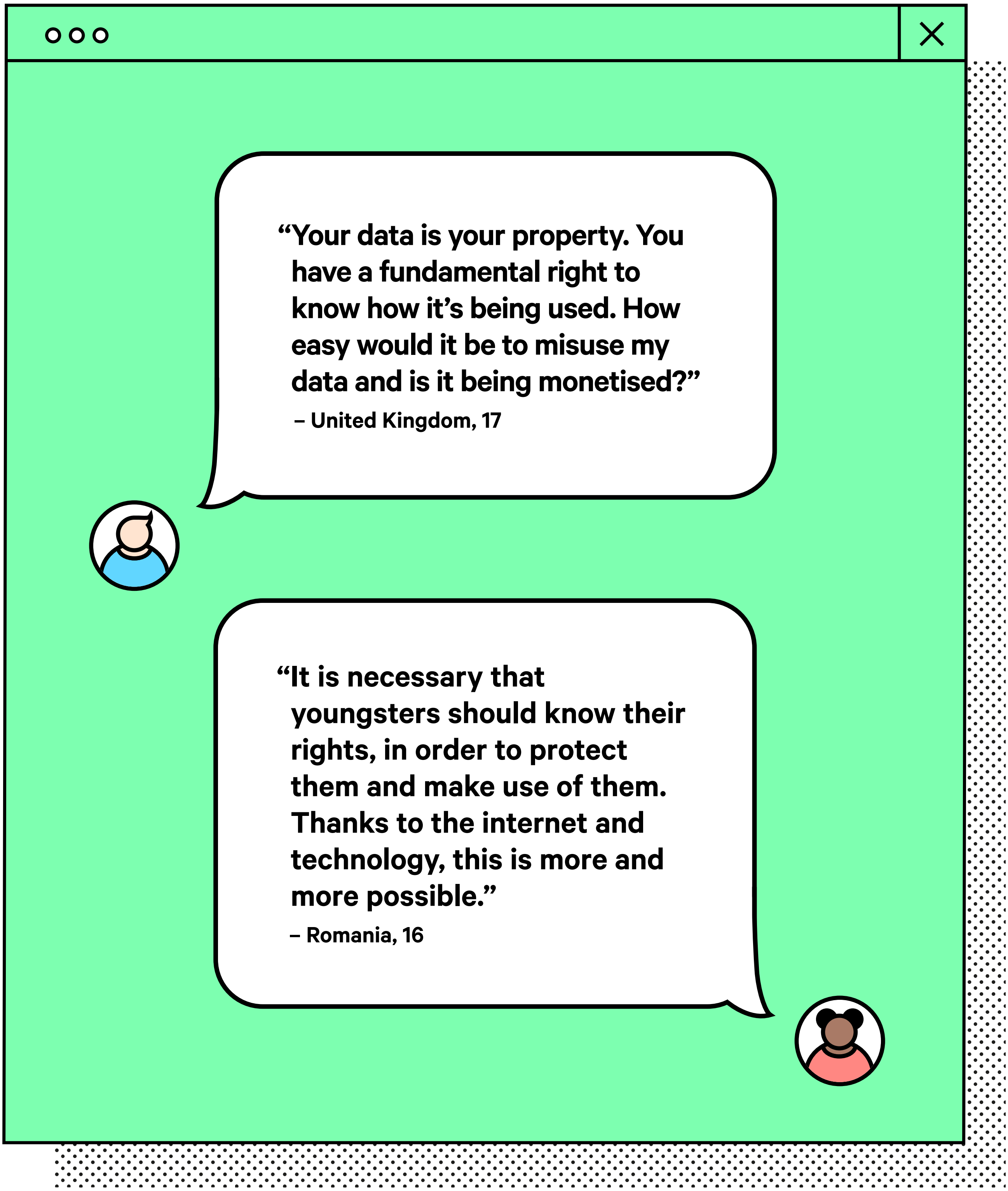
[322] Child Online Safety Universal Declaration, Broadband Commission, 2019.

[323] Notice and Takedown: Company policies and practices to remove online child sexual abuse material, United Nations Children's Fund and GSMA, 2016.

[324] Virtual Global Taskforce, Virtual Global Taskforce, 2016.

[325] Law enforcement - Internet service provider Cooperation, Council of Europe, 2007.

< PREVIOUS SECTION NEXT SECTION >



“Your data is your property. You have a fundamental right to know how it’s being used. How easy would it be to misuse my data and is it being monetised?”
– United Kingdom, 17

“It is necessary that youngsters should know their rights, in order to protect them and make use of them. Thanks to the internet and technology, this is more and more possible.”
– Romania, 16

SYSTEM FOLDER

8 ITEMS | 105 MB IN DISK | SECTION 6

< PREVIOUS SECTION NEXT SECTION >

Key documents

The UN Convention on the Rights of the Child and related documents:

1. **UN Convention on the Rights of the Child**[326]
   Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20November 1989; entered into force on 2 September 1990, in accordance with Article 49.

   There is also a child-friendly Convention on the Rights of the Child text and graphics (see also 'Why Children's Rights Matter' section) to help children understand their rights.

2. **Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography**[327]
   Adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000; entered into force on 18 January 2002.

3. **Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict**[328]
   Adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000; entered into force on 12 February 2002.

4. **Optional Protocol to the Convention on the Rights of the Child on a communications procedure**[329]
   Resolution adopted by the General Assembly on 19 December 2011.

5. **UNICEF Guidance: How We Protect Children's Rights with the UN Convention on the Rights of the Child**[330]
   UNICEF's short guide to the Convention and its Optional Protocols.

6. **General comment No. 25 (2021) on children's rights in relation to the digital environment**[331]
   General comment No. 25 provides a practical analysis of the ways in which the rights contained in the UNCRC apply to child online safety and the digital world.

7. **The Young People's Version of the UNCRC General comment No. 25 (2021) on children's rights in relation to the digital environment**[332]
   This document sets out children's rights in the digital world in their words and explains their rights in an accessible way.

[326] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1995.

[327] The United Nations Convention on the Rights of the Child – The Children's Version, United Nations Children's Fund.

[328] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, Office of the United Nations High Commissioner for Human Rights, 2002.

[329] Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, Office of the United Nations High Commissioner for Human Rights, 2002.

[330] Optional Protocol to the Convention on the Rights of the Child on a Communications Procedure, Office of the United Nations High Commissioner for Human Rights, 2014.

[331] How we protect Children's rights with the UN Convention on the Rights of the Child, United Nations Children's Fund.

[332] In Our Own Words – Children's Rights in the Digital World, 5Rights Foundation, 2021.

< PREVIOUS SECTION NEXT SECTION >

Other relevant international frameworks and documents:

1. **The WeProtect Global Alliance *Model National Response* (MNR)**[333]
The Model National Response (MNR) is a key part of any national toolkit for child online safety. The MNR is focused on helping countries to build their response to online child sexual exploitation and abuse, but it indicates that this cannot be addressed in isolation. A wider set of capabilities to prevent and tackle child sexual exploitation and abuse must be in place to ensure a complete national response. This toolkit provides resources that support implementation of the MNR. The Child Online Safety Toolkit can help signatories of WeProtect Global Alliance's MNR to ensure that they have the institutional capacity to deliver on its goals, and that the obligations under the General comment No. 25 (2021) are met.

2. **ITU Guidelines on Child Online Protection**[334]
The ITU Guidelines on Child Online Protection are a comprehensive set of recommendations for all relevant stakeholders on how to contribute to the development of a safe and empowering online environment for children and young people.

   The COP Guidelines are the product of the collaborative effort of 80 experts from different sectors – including government stakeholders, international organisations, NGOs, academia, and the private sector. First drafted in 2009, they were updated in 2020 and include four sets of guidance for:

   □ Children

   □ Parents/carers and educators

   □ Industry and

   □ Policy makers

3. **The UN Sustainable Development Goals (SDGs)**
Child online safety contributes to the achievement of several of the SDGs and may form part of policy makers' agendas to meet their commitments under the SDGs. The 2030 Agenda for Sustainable Development,[335] adopted by all United Nations member states in 2015, provides a shared blueprint for peace and prosperity for people and the planet, now and into the future. At its heart are the 17 Sustainable Development Goals (SDGs)[336] which are an urgent call for action by all countries – both developed and developing – in a global partnership. They recognise that ending poverty and other deprivations must go hand-in-hand with strategies that improve health and education, reduce inequality, and spur economic growth – all while tackling climate change and working to preserve our oceans and forests.

4. **UN Guiding Principles on Business and Human Rights**[337]
"These Guiding Principles are grounded in recognition of:

   (a) States' existing obligations to respect, protect and fulfil human rights and fundamental freedoms;
   (b) The role of business enterprises as specialised organs of society performing specialised functions, required to comply with all applicable laws and to respect human rights;
   (c) The need for rights and obligations to be matched to appropriate and effective remedies when breached.

   These Guiding Principles apply to all States and to all business enterprises, both transnational and others, regardless of their size, sector, location, ownership and structure." ▶

[333] Model National Response, WeProtect Global Alliance, 2015.
[334] Guidelines on Child Online Protection, International Telecommunication Union, 2021.
[335] Transforming our world: the 2030 Agenda for Sustainable Development, United Nations Department of Economic and Social Affairs, 2015.
[336] The 17 Goals, United Nations Department of Economic and Social Affairs, 2015.
[337] Guiding Principles on Business and Human Rights, Office of the United Nations High Commissioner for Human Rights, 2011.

< PREVIOUS SECTION NEXT SECTION >

5. **The World Health Organization's INSPIRE: Seven Strategies for Ending Violence Against Children**[338]
This is "an evidence-based technical package to support countries in their efforts to prevent and respond to violence against children aged 0-17 years. The package includes the core document describing what the INSPIRE strategies and interventions are; an implementation handbook that provides details on how to implement the interventions; and a set of indicators to measure the uptake of INSPIRE and its impact on levels of violence against children."

6. **UNICEF's Draft Policy Guidance on AI for Children**[339]
This is designed to promote children's rights in government and private sector AI policies and practices, and to raise awareness of how AI systems can uphold or undermine these rights. The policy guidance explores AI and AI systems, and considers the ways in which they impact children. It draws upon the Convention on the Rights of the Child to present three foundations for AI that upholds the rights of children:

□ AI policies and systems should aim to protect children.

□ They should provide equitably for children's needs and rights.

□ They should empower children to contribute to the development and use of AI.

Building on these foundations, the guidance offers nine requirements for child-centred AI and provides indicative resources to operationalise the guidance.

7. **Luxembourg Guidelines on Terminology for the Protection of Children from Sexual Exploitation and Abuse**[340]
The Guidelines are an initiative by 18 international partners to harmonise terms and definitions related to child protection. They aim to provide greater conceptual clarity on terminology in order to ensure stronger and more consistent advocacy, policy and laws in all languages across all regions of the world.

8. **The Precautionary Principle**[341]
UNESCO, along with its advisory body World Commission on the Ethics of Scientific Knowledge and Technology, developed a working definition of the 'precautionary principle' that is found in many international instruments relating to scientific developments in general, and which is relevant to child-centred design in technology:

"When human activities may lead to morally unacceptable harm that is scientifically plausible but uncertain, actions shall be taken to avoid or diminish that harm. Morally unacceptable harm refers to harm to humans or the environment that is:

1. threatening to human life or health, or
2. serious and effectively irreversible, or
3. inequitable to present or future generations, or
4. imposed without adequate consideration of the human rights of those affected. ▶

[338] INSPIRE: Seven Strategies for Ending Violence Against Children, World Health Organization, 2021.

[339] Policy Guidance on AI for Children, United Nations Children's Fund, 2020.

[340] Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International, 2016

[341] The Precautionary Principle, World Commission on the Ethics of Scientific Knowledge and Technology, 2005.

< PREVIOUS SECTION

NEXT SECTION >

The judgement of plausibility should be grounded in scientific analysis. Analysis should be ongoing so that chosen actions are subject to review. Uncertainty may apply to, but need not be limited to, causality or the bounds of the possible harm.

Actions are interventions that are undertaken before harm occurs that seek to avoid or diminish the harm. Actions should be chosen that are proportional to the seriousness of the potential harm, with consideration of their positive and negative consequences, and with an assessment of the moral implications of both action and inaction. The choice of action should be the result of a participatory process."

9. **Regional frameworks for the protection of children's rights**
   For example, the Council of Europe's Guidelines[342] to respect, protect and fulfil the rights of the child in the digital environment provide helpful guidance in the European context. The African Union developed the African Charter on the Rights and Welfare of the Child[343] to describe the rights of children in the African context.

10. **Innovative developments on the national level that are of global significance**
    For example, the UK's Age Appropriate Design Code[344] and the Australian Online Safety Act.[345]

[342] Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Council of Europe, 2018.

[343] African Charter on the Rights and Welfare of the Child, African Union, 1990.

[344] Introduction to the Age Appropriate Design Code, Information Commissioner's Office.

[345] Consultation on a Bill for a new Online Safety Act, Department of Infrastructure, Transport, Regional Development and Communications.

○○○ SYSTEM FOLDER ✕

8 ITEMS	105 MB IN DISK	SECTION 7

< PREVIOUS SECTION NEXT SECTION >

Glossary

At its 86th session, the Committee on the Rights of the Child adopted its General comment No. 25 (2021) on children's rights in relation to the digital environment. This terminology glossary was also included as part of this, and is not exhaustive.

Assistive technology
Technology developed to support or improve an individual's independence, including adaptive and rehabilitative systems and devices for people with disabilities such as a screen reader or speech recognition.

Automated processing
The process of making a decision by automated means, i.e. using software configured to analyse the data provided and to follow set rules to reach decisions based on algorithms, without human involvement.

Automated search
The process of assessing user data to filter the content they access online, primarily for commercial interests. Content is usually chosen based on perceptions of the user's reaction to other content, or based on content that other users who acted in similar ways went on to seek out.

Automated systems
Software and hardware programmed to perform a function automatically without the need for human intervention to provide inputs and instructions for each operation.

Behavioural targeting
Analysing users' online activity in order to target them with advertising, messaging, suggestions for further content or contacts with other users based on their previous preferences, often with the intention to manipulate their future behaviour.

Content risks
Potential harm to users based on the nature of online content, including age-inappropriate (e.g. pornography), unreliable (e.g. misinformation or disinformation) or certain other categories of content (e.g. promoting risky behaviour or methods of self-harm or suicide).

Contact risks
Potential harm created by the opportunity for users to contact each other using online services, e.g. enabling strangers or people hiding their identity to contact children.

Conduct risks
Potential harm based on the behaviour or conduct of the user or their peers, e.g. deliberately using online platforms to threaten or harass other users, including cyberbullying, "sexting" and hateful comments, sometimes also unintentionally by disclosure of private information of other users.

Contract risks
Potential harm wherein a user is exposed to inappropriate commercial contractual relationships or pressures, e.g. compulsive use, gambling, targeted advertising, hidden costs, unfair terms and conditions, and loss of control of personal data.

< PREVIOUS SECTION NEXT SECTION >

Content moderation
The practice of monitoring and reviewing user-generated content against pre-determined rules to remove content deemed impermissible, either automatically or using human moderators. Content moderation can be performed simultaneously with content generation, as in chat services or with a time delay, as in forums.

Cyberaggression
Acts of harm enacted by individuals or groups, online or through the use of digital technology, often with the intention of causing offense or hurt to another individual or group.

Data minimization
The principle of only collecting the minimal amount of relevant personal data necessary to the purpose for which it is being processed, and retaining that data only so far as it is necessary to the purpose.

Data processing
Includes processes of data collection, recording, retention, analysis, dissemination and use.

Digital literacy
The ability to use information and communication technologies to find, evaluate, create, and communicate. Related terms include 'media literacy', 'information literacy' or 'media and information literacy', among others.

Digitization
The adaptation of environments, practices, businesses and daily life to include and benefit from digital services and infrastructure. This also refers to the conversion of information into a digital format.

Disinformation
When false information is knowingly shared.

Emotional analytics
The collection of data to determine or infer an individual's mood, often conducted by assessing video, voice and written communication, or personal data, to identify markers such as facial expression and tone that are correlated with specific emotions using machine learning techniques including algorithms.

Identity theft
The fraudulent impersonation of another individual, e.g. in order to access their wealth, damage their reputation, gain access to their online contacts or otherwise profit.

Immersive advertising
The seamless integration of advertisements into online content or digital services, allowing users to remain immersed in the content and services features whilst simultaneously being exposed to brand marketing and messaging.

Implant technology
A microchip that can be implanted into a person to store, track or retrieve information contained in an external database, such as personal identification, and/or medical or law enforcement or contact information.

Information filtering
The use of a programme to screen digital content and identify or hide content that matches set criteria. Common uses of information filtering include hiding offensive content from appearing in search engine results, or sorting which results appear first.

Misinformation
When false information is shared, but no intentional harm is meant.

< PREVIOUS SECTION NEXT SECTION >

Neuromarketing
The study of how people's brains react to marketing content, and the application of this in developing more effective marketing campaigns. Reactions can be measured in a wide range of ways, from brain activity scanning to engagement time, click-throughs and time spent on a website.

Privacy-by-design
The practice of designing online services with the aim of protecting users' privacy as much as possible, e.g. by setting the accounts of underage usersto be private-by-default or by minimizing the amount of data collected.

Profiling
The practice of using an individual's personal data to infer, predict or analyse characteristics about that person, e.g. their likes, dislikes, preferences, views, opinions or behaviour, to recommend content, products or services based on the person's data profile.

Safety-by-design
The practice of designing online services with the aim of ensuring users' safety as much as possible, e.g. by default safe settings for accounts of underage users or by preventing adults from contacting underage users.

Targeted advertising
The practice of showing particular adverts to users based on data collected about them, e.g. their online activity, purchases, location, gender, age, preferences, etc.

Virtual reality & Augmented reality

Virtual Reality:
The computer-generated simulation of a three dimensional image or environment that can be interacted with in a seemingly real or physical way by a person using special digital equipment, such as a helmet with a screen inside or gloves fitted with sensors.

Augmented reality:
A simulation of the physical world with altered characteristics or supplemented items, usually experienced through a screen to enable the overlay of virtual objects over a live image or video of reality.

For further terms specifically relating to child sexual abuse, please refer to ECPAT's Luxembourg Guidelines.[343]

[343] Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International, 2016.

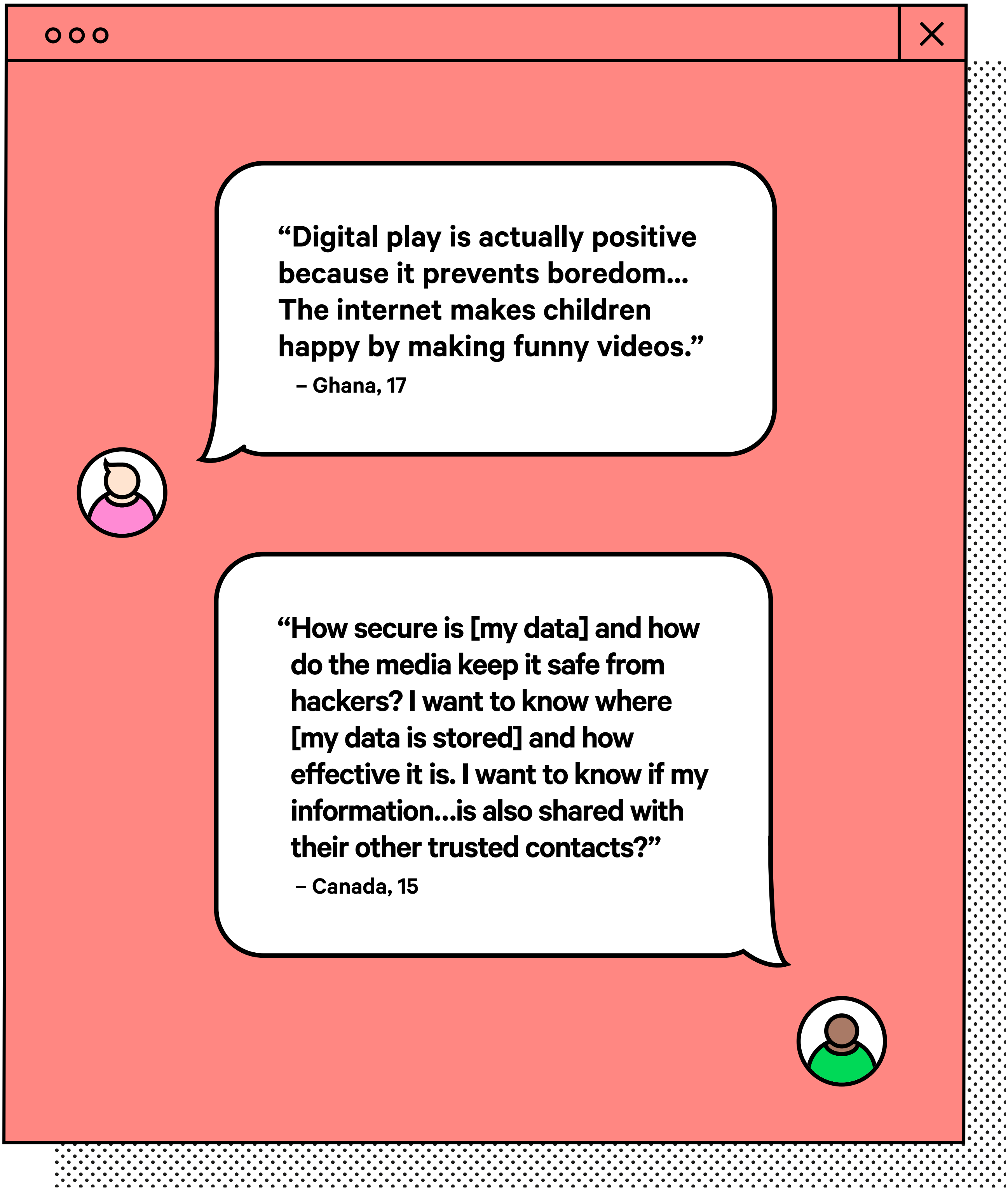
< PREVIOUS SECTION NEXT SECTION >

Afterword

Making child online protection a reality is the work of many: world leaders, the international community, policymakers, the enforcement community, health professionals, teachers, parents, carers and children.

< PREVIOUS SECTION

NEXT SECTION >



"Digital play is actually positive because it prevents boredom... The internet makes children happy by making funny videos."

– Ghana, 17

"How secure is [my data] and how do the media keep it safe from hackers? I want to know where [my data is stored] and how effective it is. I want to know if my information...is also shared with their other trusted contacts?"

– Canada, 15

○ ○ ○ SYSTEM FOLDER ✕

8 ITEMS | 105 MB IN DISK | SECTION 8

Draft model policy

The following text is a draft model policy, bringing together all the sections of this Toolkit. Each country has its own starting point when drafting their child online safety policy. This model provides a way to address the digital dimension of children's rights.

Introduction

Why children's rights matter

Children's rights provide a thread which runs through all policy that affects children's lives, both online and offline. The aim of a child online safety policy is, fundamentally, to make children's rights to protection and participation real and effective as they engage with the digital world.

Children and their families have human rights under the International Bill of Rights, including the Universal Declaration on Human Rights 1948, the International Covenant on Civil and Political Rights 1966 and the International Covenant on Economic, Social and Cultural Rights 1966, as well as regional and national human rights structures.

Specific to children, the United Nations Convention on the Rights of the Child 1989 ('the Convention' or CRC)[1] along with its Optional Protocols on the Sale of Children[2] and Children in Armed Conflict[3] provide a practical framework for understanding how human rights apply to children. The Convention is the most widely ratified human rights treaty in history and its Optional Protocol on a Communications Procedure helps to make it enforceable so that children's rights are real and effective.

All rights contained in the CRC are relevant to child online safety, and consulting children is crucial to understanding what those rights mean in practice. For example, children's rights to play, participation and to family life in the online space should be considered. All those involved in carrying out consultations should be properly trained on children's rights and what children's voices and inclusion means in practice.

5 key considerations

1. Identifying risk and mitigating harm

Child online safety strategies must be developed primarily to maximise the benefits children can gain from digital technologies. This necessarily means that there is a prime responsibility to mitigate risks, minimise the likelihood of harm occurring, address harms where they have occurred, and consider how products and services may impact the end user, if that user is (or is likely to be) a child. Designing products and services that anticipate the safe participation of children is key.

While acute harm is suffered by some children, millions of others experience online harm in one form or another. For example, there is a wide range of risks from commercial surveillance or exploitation, exposure to falseinformation or scams, predators or bullying, while a lesser number suffer the acute harm of child sexual abuse. Many risks are cumulative. These impact different children in different ways and one form of harm may offer gateways to other forms of harm.[4]

The global nature of the online world means children face many of the same online risks regardless of their own geographical location. But different contexts can also raise specific concerns. In some cases, a child may be disadvantaged by a lack of access to the online environment; in other cases, there may be a link between harm that happens online with a child's offline experience. Specific risks and harms often overlap with each other. There are very few straight lines or neat divisions.

[1] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989.

[2] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989.

[3] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989.

[4] Building the digital world that young people deserve, 5Rights Foundation, 2020.

Factors such as gender, age, family circumstances, socioeconomic status, location, experiences and availability of digital technology, can alter the risks and the ways in which children experience harm. Some risks and harms affect whole communities and classes of children: for example, girls attract higher levels of abuse but for boys the abuse tends to be harsher.[5] Cultural norms surrounding masculinity also worsen the problem of under-detection and under-reporting of male child sexual abuse.[6] Risks and harms may also be amplified by platforms which are designed in a manner that encourages the sharing of shocking and sensational content – or they might profile or promote certain types of user behaviour because this drives profitable engagement.

Policymakers must consider all risks to children and take steps to mitigate them. A key tool to identify risk is The 4Cs framework.

The CO:RE 4Cs classification recognises that online risks arise when a child:

- Engages with and/or is exposed to potentially harmful **content**
- Experiences and/or is targeted by potentially harmful **contact**
- Witnesses, participates in and/or is a victim of potentially harmful **conduct**
- Is party to and/or exploited by a potentially harmful **contract.**

2. Promoting access, accessibility and inclusion

Today, access to the online world is crucial for children to realise their rights and achieve their full potential. A child online safety policy must be inclusive, both in aspiration and in practice.[7] This means that it must be adequately resourced and should build on existing best practice and frameworks, particularly in situations where resources are limited. Whether implementing child online safety policy means adapting existing legislation (e.g. regarding child protection, consumer protection or telecoms regulation) to the child online safety context or creating new bodies of law, it must promote inclusion and equality for all children, no matter who or where they are.

Children are not a homogeneous group. Child online safety policies must be accessible and inclusive to reach all children, whoever and wherever they are. A "digital divide" is very likely to arise where some children have easy access to the online space, while others are effectively excluded. Frameworks need to be age appropriate and work for all children regardless of gender, race, religion, nationality, ethnicity, disability or any other characteristics. Language should be accessible and inclusive and, where needed, materials should be available in a range of different languages. Child online safety materials should be developed in consultation with children and parents/carers: at a minimum, they should be age-appropriate, gender-neutral and easily accessible to children of different ages and their parents/carers. Where literacy is limited, visual materials will often get messages across much more effectively. Using consistent terms across platforms helps to make child online safety more easily understandable and accessible for children and their families and carers.[8]

Policy-makers must ensure they are promoting access for children online and including them in their journey in making digital environments safe.

[5] Safe Online Investment Portfolio Results 2020, Global Partnership to End Violence against Children, 2020. p.2.

[6] Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse, Global Partnership to End Violence against Children, 2021. p.68.

[7] For example: children with disabilities or children from marginalised minority groups, street children, displaced children and migrant children, among others. This issue is further discussed in the cross-cutting themes below. More information on the model and the checklist can be found in 'Voice' is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child, Laura Lundy, 2013.

[8] See introduction on the importance of language and definitions and glossary section.

3. Building a chain of responsibility

The responsibility for child online safety involves many people, specialisms and organisations – including government, law enforcement, business, educators, psycho-social support, families, and children. Some links in the chain bear a greater weight of responsibility.[9] For example, a service that is likely to be accessed by or impact on children should consider if any of its features pose a risk to children. They should do this before engaging with any child users. This is often referred to as 'safety by design', or 'child-centred design'. Safety by default should be the norm.

Taking responsibility for child online safety includes both preventing the harm before it happens and taking action when things go wrong. Complaint and reporting mechanisms need to be accessible and clearly signposted so that children, carers and professionals who need them can find and use them easily. Within online business systems, mechanisms should be put in place which allow for reports of complaints to be monitored and evaluated so that areas of concern can be swiftly identified and addressed.

Laws and regulations need to establish clear frameworks for prevention and responsibility and redress when things go wrong. This includes collecting data about reports and complaints, so that they are monitored and analysed to improve the system. Children and parents/carers should not be made responsible for preventing or addressing risks and harms that they have little understanding or control over. Consent cannot be used to absolve public or private organisations from their responsibilities regarding child online safety. Integrating child online safety into existing frameworks for product safety[10], child protection[11], children's rights[12] and consumer rights[13] may help to avoid gaps in responsibility and duplication of resources, roles and responsibilities. There should, and must, be no legal loopholes that undermine effective child online safety.

It is vital that child online safety is embedded and integrated into all related policy areas, from national broadband plans to education curricula, in a way that is transparent, accountable and enforceable. Creating silos can lead to regulatory conflict and fragmented policy making and implementation.

4. Integrating child centred design

Child online safety must be embedded in the design and development of technology. Child-centred design builds child online safety into services and products from the outset. This should include ensuring that child online safety is considered in the regulatory requirements for design and in the licensing of new technologies[14]. Child-centred design may also be referred to as safety/rights/privacy/ethics by design.

Applying the precautionary principle[15] to technology that may impact children and young people ensures that child online safety is considered at an early stage. UNESCO's World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) put forward a 'working definition' of the precautionary principle:

"When human activities may lead to morally unacceptable harm that is scientifically plausible but uncertain, actions shall be taken to avoid or diminish that harm.

[9] See for example the UN Guiding Principles on Business and Human Rights.

[10] Child Protection Hub, European Commission, 2021.

[11] Strategy for the Rights of the Child, Council of Europe, 2021.

[12] Consumer rights directive, European Commission, 2014.

[13] Guidelines for policy-makers on Child Online Protection, International Telecommunication Union, 2020.

[14] Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, GOV.UK, 2021.

[15] See Communication from the Commission on the precautionary principle, EUR-Lex, 2000; The precautionary principle: Definitions, applications and governance, European Parliament, 2015.

Morally unacceptable harm refers to harm to humans or the environment that is:

- Threatening to human life or health, or
- Serious and effectively irreversible, or
- Inequitable to present or future generations, or
- Imposed without adequate consideration of the human rights of those affected."[16]

The precautionary principle should guide a framework for safety and privacy by design to ensure child online safety and children's rights are incorporated in technology at the design stage. Child-centred design should not only be an ethical concept, but a legal requirement.[17] It should also be incorporated into criteria for funding research and development that may affect children's rights online.

Technology and artificial intelligence (AI) have the potential to improve child online safety and to protect children's rights. Support for the development of technological tools to realise children's rights and enhance child online safety is an important aspect of a child online safety policy. The wider impact of AI or other technology designed to protect children must be assessed in light of all children's rights[18] to avoid undermining other rights such as privacy and non-discrimination.

Children themselves are extremely diverse and the full range of children's characteristics, backgrounds and contexts should be considered in the development, implementation and monitoring of the effectiveness of policies in this area. Effective action on child online safety needs to address perceived tensions. For example, in debates on encryption, advocates for protection from child sexual exploitation and abuse (CSEA) may find their arguments clash with those related to privacy and data protection. Such conflicts must be resolved to the extent that there is a practical outcome, to avoid many years of cyclical debate while children are put at risk or come to harm. In such cases, the 'best interests' of the child should be paramount.[19]

There are several frameworks and processes that support the application of child-centred design in policy making, including the Precautionary Principle, Child Impact Assessments[20] and Consultation with Children.[21]

In addition, the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) introduced a standard containing practical steps that companies can follow to design digital products and services that are age appropriate,[22] and the Digital Futures Commission has set out how children's right to play freely could be supported in a digital world by improving the design of digital products and services. Policy makers should always seek to ensure that products and services minimise risk before they are made available to children.

Safety by design, and rights by design are systemic in nature and therefore aim to protect millions of children from the outset, not after the fact.

5. Ensuring effectiveness

Child online safety and children's rights in the digital environment can only be truly effective through practical policy actions, adequate resourcing, and enforcement.

[16] The Precautionary Principle, World Commission on the Ethics of Scientific Knowledge and Technology, 2005.

[17] See for example Article 25, General Data Protection Regulation, European Union, 2018.

[18] See for example General comment No. 25 (2021) on children's rights in relation to the digital environment, UNCRC, 2021.

[19] Convention on the Rights of the Child, Office of the United Nations High Commissioner for Human Rights, 1989. (See in particular Article 3, Section 1 on children's rights).

[20] Child Rights Impact Assessment, Digital Futures Commission, 2021.

[21] Child Rights Impact Assessment, Digital Futures Commission, 2021.

[22] IEEE 2089-21 Standard for Age-Appropriate Digital Services Framework, IEEE SA, 2021.

Child online safety is relevant to a wide range of policy areas, including information and communications technology (ICT), education, criminal justice, health, regulation of industry, social and family support, business, human rights and equality, international development, and many others.
Cooperation across different ministries and agencies working in policy areas is thus essential for effective action on child online safety. Budgeting in order to resource the policy both within and across different departments will be necessary. A policy with insufficient funds, or a partnership with no capacity, i.e. something which exists only on paper, will not result in effective child online protection.

Understanding effectiveness means reviewing the impact of child online safety policies. Monitoring, evaluation and data collection are key to informing good policy development. Learning from and sharing lessons on effective policy making across borders is an efficient way to maximise effectiveness. Checking the effectiveness of child online safety policy requires consultation not only with the key actors involved, but also with children, to understand how actions are affecting them or could impact on them in the future.[23] It is an ongoing process.

Policy should be data-driven and evidence-based. Both relevant authorities and private companies should be required to collect and share data to aid understanding of child online protection issues, in compliance with data protection laws and principles. Child online safety is a relatively new policy area, so where evidence is not available or contested, policy-makers should take a precautionary approach, or look to other contexts and take a 'what works' approach – for example, with health and safety principles, or frameworks such as INSPIRE: Seven Strategies for Ending Violence Against Children.[24]

Child online safety is not a standalone issue. The effectiveness of child online safety policy will depend on the overall effectiveness of key institutions and their ability to collaborate towards effective protection.
Ensuring effective accountability for child online safety overall, and the prevention of CSEA in particular, relies on strong domestic justice systems. The Model National Response (MNR) presents guidance on this issue.

Effective approaches to child online safety also rely on adequate resourcing for the institutions that support them, including in areas such as psycho-social support, and regulation in ICT and related fields. Upholding children's rights effectively through child online safety policy depends on efficient human rights legislation and specific legislation and regulation with oversight bodies to guarantee children's rights in both the online and the offline environment.

Policy makers should ensure that the institutional capacity, the resources, and accountability mechanisms are in place to support child online safety policies. Where conflicts arise, the 'best interests' of children should be paramount. Without these, even the best policies will be ineffective.

Policy action areas

1. Institutional capacity

1a. Affirm public commitment to child online safety at the highest level
National leaders, including the Prime Minister or President, should commit to child online safety on both the national and international stages.

1b. Designate a ministry or agency to take the lead on developing the national child online safety policy
Around the world, a range of different agencies and ministries lead on child online safety policy, and the choice of agency or ministry may affect the way a child online safety policy evolves and prioritises different aspects of child online safety. Child online safety is likely to sit across several ministries, but it is important that a lead agency owns the agenda. In some countries, child online safety policy is led by the ministry responsible for ICT, in others the ministry responsible for children and families, and yet in others, the Ministry of Justice. It may be that where existing groups are working on violence against children (VAC) or cybersecurity, they can be extended to include the necessary expertise in order to prevent siloed working. The lead agency may be chosen for its authority, expertise, resources, capacity or enthusiasm – but any lead agency will have to work with others. Whichever ministry takes the lead, it must commit to a holistic approach that reflects the overarching needs of child online safety.

[23] Digital Futures Commission, 5Rights Foundation, 2021.

[24] INSPIRE Indicator Guidance and Results Framework, World Health Organisation, 2018.

1c. Publish a definitions and language manual
The designated lead ministry should publish a full list of definitions and language that reflects definitions used in international best practice.[25]

1d. Establish a National Child Online Safety Steering Committee
The National Child Online Safety Steering Committee will be responsible for policy implementation and development and will serve as a focal point for national and regional cooperation. It will be responsible for taking the Child Online Safety Toolkit and developing the strategy to implement it – this might be called the action plan. The Committee will address a broad set of competencies that cover various policy areas, including education, health, justice, consumer protection, data protection, law enforcement, ICT, and family and children's services, among others, and will supervise implementation and uphold standards. The Committee should be formally required to cooperate with all those who have a remit for child safety or cybersecurity, and should report regularly to the lead ministry.

1e. Understanding child online safety stakeholders
The enforcement community, business, third sector, children's rights organisations, educational institutions, parents/carers and academia all hold useful insights and important interests in child online safety. In some contexts, creating a stakeholder group may be useful to support the Committee with its activities and ground its action plan in real-life scenarios. In other contexts, informal discussions or calls for evidence from an open network of stakeholders may be more effective. Either way, the National Child Online Safety Steering Committee should seek to engage with key stakeholders who can support their activities. Interagency cooperation should be promoted. The purpose of stakeholder engagement is to focus on implementation, not policy development.

1f. Define roles and responsibilities of stakeholders
There should be a co-regulatory framework that defines the roles and responsibilities of all organisations developing and managing digital infrastructure, networks and services, and the duties of government departments. Minimum standards should be established for all in the value chain, including those responsible for infrastructure, hardware, and digital products and services, and those who manage or use them when they interact with children. These standards should focus on child safety and the full realisation of children's rights in the digital world. Civil society participation and child consultation should be ensured in stakeholder groups.

1g. Define performance indicators and evaluation
Each aspect of the implementation plan should have a corresponding accountable authority (person, institution, body) and human and financial resources to successfully complete the task envisioned. It may be that the same authority is responsible for more than one policy area, or a single area of expertise. Key Performance Indicators (KPIs), evaluation mechanisms and clear reporting structures should be introduced to enable the Steering Committee to oversee and manage progress. As the digital environment evolves rapidly, KPIs will require constant review.

1h. Ensure integration of child online safety across government policy areas
Any relevant national plans, such as a National Broadband Plan or digital literacy framework, should include child online safety policy as part of the rollout strategy. Plans that take place over several years should be checked at key milestones.

2 Legal and regulatory frameworks

2a. Strengthen and enforce laws that prohibit child online safety-related offences
Criminal laws and procedures facilitate the investigation and prosecution of online offences that violate children's right to protection and should be strengthened and amended in line with international standards and best practices. This should include the introduction of mandatory risk assessments to reduce potential for harm, enhancing sanctions and sentencing frameworks where necessary. It should also include the potential for notice and takedown procedures. Criminal laws concerning child online safety should be developed in light of all children's rights, including their right to be heard and to participation.[26]

[25] See for example, Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International, 2016.

[26] For example, legal frameworks that do not make it clear whether self-generated sexual images that are exchanged on consensual basis between children will be considered illegal Child Sexual Abuse Material. Even if children are not prosecuted in practice this legal uncertainty with potential criminalisation may undermine trust, control and autonomy rights.

2b. Introduce data protection regulations and independent supervisory authorities, ensuring that children's data is protected appropriately, and collected only where necessary with high levels of security and care
Such general regulations should include special category status for children's data, requiring higher levels of protection and safeguards by default as well as protections against the inappropriate commercial use of children's data. Where consent is sought from children, or parents/carers on their behalf, for the online collection and processing of younger children's data it must be informed and meaningful. Data gathering for safeguarding purposes should be given special consideration in exceptional circumstances where this is in the best interests of the child.

2c. Strengthen criminal investigation, prosecution and sentencing for online child sexual exploitation or abuse[27]
Criminal justice agencies with responsibilities for child online safety-related offences should be trained in child online safety issues with the aim of driving greater prevention, successful prosecution and appropriate sentencing as well as greater understanding of the impact on victims. The capabilities of relevant investigation and response teams should be reviewed and strengthened to detect, prevent and respond to cybersecurity threats, specifically those related to child online safety. Criminal justice systems should be able to ensure timely access to justice.

2d. Review and strengthen youth justice systems
Ensure that the law is clear and proportionate to minimise the risk of children coming into conflict with the law in the context of child online safety. Where children face criminal sanctions related to child online safety, for example in relation to cyberbullying or image-based sexual abuse, the justice system must make every effort to prevent children from being criminalised and provide adequate support and legal representation to those children who come into conflict with the law to protect their rights.

2e. Identify and ratify child online safety-related international treaties & protocols
Building a sustainable ecosystem of child online safety requires a multi-stakeholder approach and participation on a global scale. Each country should identify and ratify relevant international and regional protocols and treaties and take steps to implement their measures.

2f. Strengthen the capacity of law enforcement agencies
Shortcomings in enforcement and the judiciary will be identified, and measures will be put in place to increase awareness, reporting and successful prosecution. International training and skills sharing should be sought where possible, and cross-sector coordination and collaboration between industry and law enforcement should be encouraged.

3 Personal data and identity

3a. Establish or ensure existing data protection frameworks are effective in providing specific protection for children's data
Children's rights in the online environment are intimately connected with the way their data is collected, stored and used. Data protection law and regulation for children must be accessible, effective, and capable of evolving to meet emerging risks.[28]This means, not only establishing the legal and regulatory frameworks, but also making sure they work in practice and are implemented accordingly.

3b. Establish protocols for and limitations on the use of automated decision making that may affect children
Standards, laws and codes of practice should ensure that children benefit from automated systems and are not penalised through automated decision making.[29] It is particularly important to avoid the potential for discrimination through automated decision making. These protocols and limitations may apply in the context of criminal justice, social welfare, health and medicine, education, and the private sector among others.

[27] Child sexual exploitation and abuse (CSEA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline.

[28] General Data Protection Regulation, European Union, 2018.

[29] World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert, Office of the United Nations High Commissioner for Human Rights, 2019.

3c. Ensure adequate legal and regulatory protections for children's biometric data
Government and regulators should establish appropriate legal and regulatory protocols for and limitations on the use of children's biometric data in light of the principles of children's rights, purpose limitation and the requirements of child online safety policy.

3d. Establish clear guidance, laws and regulations on practices that may affect children's agency
Create legal frameworks preventing personalised targeting and tracking of children for commercial purposes based on their personal data. Establish codes on the use of recommendation systems and other automated decision-making processes or technologies that may drive children's behaviour, mould preferences and opinions, undermine reputations or limit experimentation.[30]

3e. Establish effective oversight and monitoring
Creating bodies and systems that can gather information relevant to child online safety and ensure transparency and effective implementation of children's rights and protections by business, government and other organisations.

3f. Establish frameworks to ensure transparency
Oversight should be provided by an appointed regulatory body that is sufficiently resourced and has the necessary capacity and expertise to understand the systems in use and how they impact on children's rights. The oversight body should also have access to independent researchers and experts.

4 Response and support systems

4a. Notice and takedown
Government institutions will work with experts, the enforcement community and industry to establish and monitor effective protocols for the notice and takedown of illegal and harmful material. Among other things, this will require the development of protocols to ensure, and legislation to permit, local internet service providers (ISPs) to restrict access to hosts that fail to take down notified content or persistently breach laws or other regulatory requirements on child online safety.

4b. Establish processes for offender risk management in relation to CSEA
An effective multi-stakeholder offender management process should be established, drawing upon international standards of good practice. Law enforcement and other criminal justice practitioners will be trained to recognise and investigate offending behaviours. Offender risk management is an essential component of child online safety, as individuals or groups of offenders can reach large numbers of child victims online.

4c. Provide adequate resources for psycho-social support for primary and secondary child victims and their families
Organisations training practitioners in the mental health, psychology and social work fields who work with vulnerable children must be required to have a basic understanding of child online safety issues.[31] Child online safety should be integrated into broader child safety and protection systems, such as safeguarding in schools or violence against children (VAC).

4d. Establish victim detection and protection frameworks
A key aim in the prevention of online harm will be to consider the needs of vulnerable children and how best to support them. One Stop Centres act as an initial umbrella institution for victims of abuse: these provide access to a range of essential services, from medical to legal support, in one centralised location. They offer a framework for safeguarding and child protection procedures, provide support for victims, and rapidly escalate reports of online crimes to the relevant authorities.[32]

[30] See for example, YouTube Data Breach Claim, McCann vs Google, 2021.

[31] What Works to Prevent Violence Against Women and Girls Evidence Reviews Paper 3: Response mechanisms to prevent violence, What Works, 2015. p.28.

[32] Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, WeProtect Global Alliance, 2016.

4e. Ensure relevant frameworks do not criminalise children
It is important to establish appropriate frameworks for managing children who may find themselves in conflict with the law in the context of child online safety – for example, in cases of cyberbullying, spreading malicious information or hacking. Where possible, children should be diverted from the criminal justice system, and opportunities for counselling or restorative justice should be preferred. Particular care should be taken to ensure that a child's circumstances are fully understood. For example, a child's behaviour might be the product of bullying, grooming or some other form of coercion.

5 Business and children's rights:

5a. Implement safety, rights, and ethics by design
Standards and codes of practice should be developed which require product designers, manufacturers and service providers to uphold children's rights and to contribute to children's online safety and security. Terms and conditions should reflect the child's best interests. Among other things, standards and codes of practice will aim to prevent children from being offered harmful or inappropriate content or contact; to protect children's online privacy on the system- or device-level; and to address security concerns raised by the Internet of Things – connected toys and services with a streaming function – to ensure that private companies have considered, through a Child Impact Assessment, a risk and mitigation process that leads to offering children an age-appropriate service.

5b. Introduce minimum standards[33]
Industry has a responsibility to ensure that children are afforded protection online. This means creating a safe and accessible online space for children, not just preventing access to harmful content. Businesses will be required to show what procedures and special considerations they have undertaken to ensure child safety and respect for children's rights – using the 4C risk framework[34] – as they develop and establish their online services.[35] A code should be created by the lead ministry or agency, overseen by the Steering Committee. These standards will be mandatory and enforceable.

5c. Application of age-rating classification
The application of consistent age-rating classification of commercial content, public service media and games and activities online offers a transparent and effective approach to managing content and services that impact children. This may be required for relevant goods and services and for content that is suitable for different age ranges. Age assurance or creating adult-only spaces will be required for prohibited content or activities that are not suitable for children. This may include providing content filters to block unwanted content.[36]

5d. Introduce moderation and reporting systems
Mechanisms to identify upsetting or unsuitable content will be required of the service providers, and transparent and robust monitoring systems must be in place for all online services, including the provision of takedown mechanisms. A free public hotline will be available for reporting and accessing specialist support and advice. Reporting mechanisms should be easily accessible for children. Flagging systems should be considered as an additional tool.

5e. Ensure protection of children from commercial pressures
Efforts to protect children from commercial pressures will include: promoting age-appropriate design; disabling targeted advertising and third-party sharing; and raising awareness of the context in which children grow up. Products and services that enhance children's rights and safety online may be certified, and action may be taken against developers of products and services that violate these values.

5f. Ensure that child-centred design principles are introduced to minimise child online safety risks
This includes, for example, the potential for introducing adult strangers to children, or targeted advertising for gambling or the recommendation of harmful content. Child online safety needs to beembedded at the design stage to prevent issues arising further down the line.

[33] See, for example, Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, GOV.UK, 2020.

[34] See section on Mitigating Risk and Harm.

[35] Children's Rights in Impact Assessments, United Nations Children's Fund, 2013.

[36] But how do they know it is a child?, 5Rights Foundation, 2021.

6 Training

6a. Provide training, skills development and mentoring for all involved in child online safety
From first responders to judges, all actors in the law enforcement chain, and professionals who work with children in other settings like education or health, must be aware of child online safety. They should be offered comprehensive training, including on how child online safety relates to their particular role, how to understand offending behaviour, and how to provide access to victim support.

6b. Provide specialised training for psycho-social support and identification of signs of the full range of child online safety issues
To be effective, relevant practitioners must be provided with child online safety training, training on safeguarding and child protection policies, and training on child and family counselling. Child online safety awareness should be incorporated into existing frameworks for child protection. Professionals working with children in education, health, community and other settings should be trained to recognise the signs and symptoms of child online safety issues.

6c. Build tertiary education schemes
Child online safety sessions should form a mandatory part of teaching, social work, health work, psychology, and other relevant degree programmes in public and private universities or education institutions. There is a need for regular review of the effectiveness of this teaching in light of advances in child online safety training and emerging issues. Curricula should cover all aspects of child online safety as laid out in this policy.

6d. Encourage professional development
Continuing education programmes on child online safety and child safeguarding for professionals working in relevant fields will be established, regularly reviewed and updated to keep pace with emerging technologies, and to address new barriers and concerns as they become apparent.

7 Education

7a. Designate child protection leads
Each school is to designate a child protection lead.[37] Each lead is to be provided with training on child protection procedures and child online safety-specific training. Leads will be responsible for ensuring that child online safety policies (including safeguarding procedures and anonymous reporting systems) are adopted, enacted and enforced in schools. The child protection lead will be the point of contact for concerns relating to child protection and child online safety, and will pass on reported harms to the relevant authorities. Leads should also facilitate intervention plans, to protect children against the full range of harms.

7b. Promote accessible digital education
Promote content, including peer-to-peer programmes, that are designed and shown to help children develop digital skills and empower children to build respectful communities that support child online safety. Digital education should be holistic and should cover data and media literacy, alongside safeguarding issues – in particular issues of sexuality and consent. Education should also be extended to parents/carers to support their role in promoting child online safety.

7c. Promote educational content
As digital adoption becomes widespread, pupils and teachers will be taught the necessary skills for interacting with digital systems to fully benefit from curriculum content, both in local and international languages.

7d. Promote data literacy
A programme of data literacy will be introduced across the school curriculum. The programme will educate children on the way their data may be used and will provide a basic understanding of the data economy. It will: emphasise and encourage the positive, autonomous and creative use of digital technologies by children; clearly define the risks, benefits, and social outcomes of using technology;

[37] This could be someone from a school safety committee, an educator or it could be someone in a village or community child protection committee where schools are represented.

and aim to ensure that protective and preventative measures are broadly disseminated, understood and applied. Data literacy education should make clear the range of stakeholders responsible for online safety.

7e. Promote critical thinking

Education for children and parents/carers on critical thinking and awareness of the risks of online disinformation should be incorporated into digital literacy education. This should include wider education to promote understanding and awareness of human rights, in particular children's rights, and the way they work online and offline.[38]

7f. Introduce formal child online safety procedures in schools

Child online safety training must form a mandatory part of teaching degrees, at both primary and secondary school level, as well as a focus of ongoing in-service training. All teachers must complete mandatory training on child online safety, be aware of school policy in relation to child online safety, and deliver child online safety lessons to students. All schools must appoint a child online safety lead to champion child online safety standards and take responsibility for enforcing school policy on child online safety.

8 Public awareness and communications

8a. Generate a public awareness programme

Awareness-raising strategies will help people understand and navigate the issue of child online safety while still benefiting from the online space. Materials to be produced should make clear the principles of child online safety and actions that can be taken to understand risk, mitigate harms, report offences and seek redress. This information will be provided in simple terms on official websites. Targeted messages and materials should be designed in consultation with children, young people and parents/carers. It should consider the specific needs of parents/carers and children, with particular attention given to the youngest and most vulnerable children – including those with learning disabilities or those without parental guidance. Peer-to-peer education is a valuable strategy for children of all ages to get to know their rights and responsibilities online. This programme of public messaging can help children and adults to understand the issues and make wise choices about their online interactions, but is not a replacement for formal education, professional training, safety by design or corporate responsibility. Such information should cover the full range of child online safety issues as set out in this policy.

The five cross-cutting themes

1. Identifying risk and mitigating harm
2. Promoting access, accessibility and inclusion
3. Building a chain of responsibility and collaboration
4. Integrating child-centred design
5. Ensuring effectiveness

The ten policy action areas

1. Institutional capacity
2. Legal and regulatory frameworks
3. Personal data, identity and autonomy
4. Response and support systems
5. Corporate responsibility
6. Training
7. Education
8. Public awareness and communications
9. Research and development
10. Global cooperation

8b. Provide accessible information and educational materials

Online safety education will start in early childhood and develop according to children's changing needs as they grow: specific materials will be produced to guide and support children of all ages, their families and caregivers. Information materials will promote the positive use of digital technology, sexuality and consent, and will consider the needs of all children, regardless of gender, age, income or background. Information provided by third parties will reflect children's rights and principles and aim to help children of all ages to get to know risks and their rights online. Materials should make clear that children and users are not responsible

[38] See Article 29 of the Convention on the Rights of the Child, and relevant sections of the general comment.

when bad things happen to them. Community groups, youth clubs, families, religious institutions and digital platforms will all be instrumental in driving effective child online safety awareness and informal education at the community level.

8c. Raise awareness of child online safety in the media
Information to support media coverage of child online safety issues in a child-friendly way should be made available. Media and entertainment companies should be made aware of child online safety and be encouraged to support public awareness campaigns where appropriate, in a balanced, responsible and informative manner. The full range of child online safety issues – not just the most dramatic headlines related to this – should be encouraged.

8d. Engage parents/carers and children in discussions about child online safety
Parents/carers and families should be empowered to understand and take action on child online safety in their own homes. Consultations with families and children are needed to identify issues, solutions and ways of raising awareness of child online safety in an effective way in the community.

9 Research and development

9a. Establish child online safety research frameworks
Countries should establish a central research fund to develop a research programme with clearly identified terms of reference and objectives that remain current, in order to enable ongoing research in child online safety across a broad range of relevant issues. Where possible, countries should reach out and cooperate with each other on child online safety research and development. Gap analysis should help to ensure resources are prioritised in areas of biggest need and to avoid unnecessary duplication. Research should be made available to regional or international partners, particularly those with the least resource.

9b. Continued innovation
Research evidence will inform the development of products and services that incorporate safety by design; enable the evaluation of child online safety practice; and provide an understanding of children's online experiences and solutions in the national context.

9c. Establish centres of excellence in research and development in child online safety
Countries should develop centres of excellence within existing institutions (universities, health settings, innovation hubs) that can share and cooperate on the development of tools, services and skills relating to child online safety through national, regional and international engagement.

9d. Establish strong ethical frameworks for research and development in child online safety[39]
Countries should develop guidelines for researchers working on child online safety, including effective consideration of children's rights as part of the research process. This should include clear guidance on data collection and the ethics and rights implications of processing children's data. The interests of the child should be the primary consideration within ethical frameworks for research and development on child online safety, including in situations of public interest access.

9e. Establish frameworks for information gathering
Regulators working in child online safety should set up frameworks for information gathering that will allow them to monitor and evaluate the effectiveness of child online safety in different contexts and the impact it has on different groups of children. Monitoring and evaluation of child online safety actions should form part of the research and development process.

9f. Enable access to private companies' data in the public interest
Frameworks should be created where social media and other companies must share their data to support research in the best interests of the child.

9g. Ensure that data and statistics are relevant to the context
Statistical models should reflect the local picture, to support the level of understanding and response to national issues. They should allow for monitoring of cross-border impacts.

[39] Children and the Data Cycle: Rights and Ethics in a Big Data World, United Nations Children's Fund, 2017.

10 Global cooperation

10a. Establish formal relationship frameworks (e.g. a Memorandum of Understanding [MoU]) with regional and global child online safety communities

Strengthening international cooperation to enhance child online safety across the globe is critical to guarantee global security. Countries should formalise collaborations for joint Public Private Partnership investments in areas related to cybersecurity, child online safety capacity building, innovation, law enforcement, the justice system and education, among others.

10b. Sign up to regional and international legal instruments that promote cooperation on child online safety

Countries should identify key regional and international instruments that will allow them to cooperate with other countries on child online safety. This should include, among other things: international agreements on law enforcement cooperation; international best practice; international programmes that may provide resources for cooperation on child online safety; and access to any human rights or related standards that will facilitate cooperation between countries.

10c. Identify partner countries and organisations that can provide appropriate models and support for child online safety development

It may not be necessary to start policy development from scratch. Countries should look for relevant examples of child online safety frameworks and tools that they may use and adapt to their own context. Sharing information on challenges and problems encountered in child online safety can be very valuable for the planning, development and implementation of child online safety policies.

10d. Support other countries developing child online safety policies

Where appropriate, share model laws, regulatory frameworks, lessons learned or other materials that can be used by other countries to develop their own child online safety frameworks and policies.[40]

[40] See for example the Australian eSafety Commissioner’s International Leadership and Collaboration Materials, 2021.

5RIGHTS
FOUNDATION

End Violence
Against Children