Executive Summary
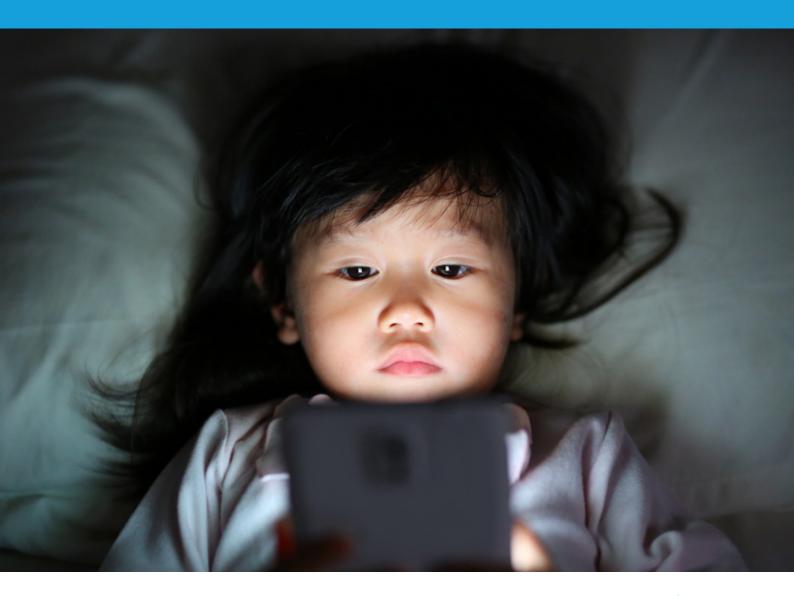# Guidelines for policy-makers on Child Online Protection
2020

Guidelines for policy-makers on Child Online Protection

2020

Introduction

The Internet has transformed how we live. It is entirely integrated into the lives of children and young people, making it impossible to consider the digital and physical worlds separately. One third of all Internet users today are children and young people, and UNICEF estimates that 71 per cent of young people are already online.

Digital technologies have opened up many new ways to communicate, play games, enjoy music and engage in a vast array of cultural, educational and skill-enhancing activities. The Internet can provide crucial access to health and educational services as well as information on topics that are important for young people but may be taboo in their societies.

However, just as children and young people are often at the forefront of adopting and adapting to the new connected technologies together with the opportunities and benefits they bring, they are also being exposed to a range of content, contact and conduct threats and harms online. It is important for policy-makers to appreciate these threats and harms in formulating policy responses.

Governments, the ICT industry and civil society need to work with children and young people to understand their perspectives and spark genuine public debate about risks and opportunities. Supporting children and young people to manage online risks can be effective, but governments must also ensure that there are adequate support services for those who experience harm online, and that children are aware of how to access those services.

Table of Contents

1 What is child online protection?

Child online protection (COP), is the holistic approach to respond to all potential threats and harms children and young people may encounter online. It is everyone's responsibility to protect children from these harms.

In context of child online protection, whilst most children will be susceptible in one form or another to online threats and harms, it is important to appreciate that some children are especially vulnerable, particularly migrant children or children living with a form of disability.

2 Preparation for a national child online protection strategy

In developing a national strategy to promote online safety, policy-makers should consider a range of aspects.

Initially they should identify and engage with the following **stakeholders** to understand their experiences, perceptions, opinions together with their existing activities and interventions.

- Children and young people
- Parents, guardians and educators
- Government Ministries
- Industry and connectivity providers
- Research and academia
- Non-governmental organizations
- Law enforcement
- Health and Social services

It is likely, across the range of actor and stakeholders, that there are already existing **activities** and actions with the objective to protect children online, but that these have occurred in isolation. It is important to understand and appreciate existing efforts in the development of the national child online protection strategy. The strategy should look to coordinate and direct efforts through the orchestration of both existing and new activities. The strategy should be included within, or cross-reference, existing national frameworks or strategy plans.

Alongside an understanding of the activities and experiences of the various actors and stakeholders, it is essential to consider the circumstances and responses from other countries. There have been innovative developments and initiatives in the regulatory and institutional response to threats to children's safety and wellbeing online. In addition to appreciating what is possible, it also helps policy-makers to challenge existing provision and potential; and identify areas of cross-border collaboration and engagement. A number of these **national and international initiatives and developments** are signposted in these guidelines.

There are clear benefits from a national child online protection strategy. The development of adequate **national legislation**, the related **legal framework**, and within this approach, **harmonisation** at the international level, are keys steps in protecting children online. These frameworks may be self-regulatory, co-regulatory or full regulatory frameworks.

3   General recommendations

With an understanding of existing national activities, interventions and frameworks together with examples from other countries, policy-makers should be in a position to start to plan for the development of a national child online protection strategy.

These guidelines include a series of recommendations that may be considered including the legal and policy frameworks.

These frameworks should address all harms against children in the digital environment but at the same time, this should not unduly restrict children's rights.

The frameworks should integrate and reference existing policy frameworks.

The frameworks should specifically cover the sexual exploitation of children online (including child sexual abuse material) as well as national education provision and expectations for industry providers.

It is important that the frameworks detail the objectives and to define the evaluation criteria.

A multi-stakeholder mechanism should be developed that defines, coordinates and drives the national activities under the direction of the national child online protection strategy. This mechanism should be the vehicle that brings together, and orchestrates, the spectrum of national actors and stakeholders.

These guidelines highlight a series of further recommendations for policy-makers to consider in developing and starting to design a national child online protection strategy.

4   A national checklist

Area	Area for consideration
Legal framework	Review the existing legal framework to determine that all necessary legal powers exist to enable law enforcement and other relevant agencies to protect persons under the age of 18 online on all Internet-enabled platforms.
	Establish, *mutatis mutandis*, that any act against a child which is illegal in the real world is illegal online and that the online data protection and privacy rules for children are also adequate.
Regulatory framework	Consider the regulatory policy development. This may include a self or co-regulatory policy development as well as a full regulatory framework.
Reporting- illegal content	Ensure that a mechanism is established and is widely promoted to provide readily understood means for reporting the variety of illegal content found on the Internet.
Reporting- user concerns	Industry should provide users with the opportunity to report concerns and issues to their users and respond accordingly.
Actors and stakeholders	Engage all the relevant national stakeholders with an interest in online child protection.

Area	Area for consideration
Research	Undertake research of the spectrum of national actors and stakeholders to determine their opinions, experiences, concerns and opportunities with regards to child online protection.
Education digital literacy and competency	Develop digital literacy features as part of any national school curriculum that is age appropriate and applicable to all children.
Educational resources	Develop Internet safety messages and materials, which reflect local cultural norms and laws and ensure that these are efficiently distributed and appropriately presented to all key target audiences.
Child protection	Ensure that universal and systematic child protection mechanisms are in place that oblige all those working with children to identify, respond and report incidents of abuse and harm that occur online.
National awareness	Organise national awareness campaigns to create the opportunity to universally highlight child online protection issues.
Tools, services and settings	Consider the role of device settings, technical tools (such as filtering programmes) and child protection apps and settings that can help.