unicef
for every child

Child Online Protection in and through Digital Learning

Considerations for Decision-Makers

Funded by
the European Union

Produced by UNICEF Regional Office for Europe and Central Asia (ECARO)

The statements in this publication are the views of the author(s) and do not necessarily reflect the policies or the views of UNICEF.

The designations employed in this publication and the presentation of the material do not imply on the part of the United Nations Children's Fund (UNICEF) the expression of any opinion whatsoever concerning the legal status of any country or territory, or of its authorities or the delimitations of its frontiers.

This product has been authored by Sarah Fuller, Education Consultant (UNICEF Regional Officer for Europe and Central Asia), under the supervision of Malin Elisson, Senior Education Adviser for UNICEF ECARO. Research support was provided by Hailey Ip, Early Childhood Development Consultant (UNICEF ECARO), and input was provided by Jessica Katherine Brown, Early Childhood Development Specialist (UNICEF ECARO) and Laura Bodendoerfer, Child Protection Specialist (UNICEF ECARO).

This guidance document is part of the programme 'Mitigation of the impact of COVID-19 on the lives of children and parents in the Western Balkans and Turkey' which has received funding from the European Union.

Cover Photo: © UNICEF/UN0460685/

This publication was produced with the financial support of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union. Its contents are the sole responsibility of UNICEF.

unicef
for every child

Child Online Protection in and through Digital Learning

Considerations for Decision-Makers

Funded by
the European Union

Preface

Three decades ago, nearly all countries committed to the UN Convention on the Rights of Child, the most widely ratified human rights convention in history. In doing so, they committed to protect children from all forms of violence, neglect, exploitation and abuse; to take all appropriate legislative, administrative, social and educational measures necessary to do so; and to ensure that the institutions and services that support children conform with these standards. Despite notable progress and continued commitment through the Sustainable Development Goals, persistent challenges remain while new ones emerge.

Recent years have seen the rapid development and proliferation of new technologies, which bring with them a host of opportunities for learning, communication, social interaction, employment and entrepreneurship. When inclusively designed and equitably distributed, information and communication technology (ICT) has enormous potential to address inequality and improve livelihoods for even the most marginalized and vulnerable children and their families. Digital technology, for example, can support access to quality learning and skills development content for children with disabilities or for young people who are out of school. Digital tools can facilitate ongoing formative assessment by teachers to enable more personalized instruction, regardless of whether learning takes place in-person or at a distance, and they can be used to help parents of young children to support their cognitive, social and emotional development at home. Digital platforms can enable educators from diverse schools, communities and even countries to connect with peers and mentors through communities of practice. On a larger scale, digitalization of education systems can improve preparedness for and resilience to crises to minimize learning disruption, as has been evidenced by the COVID-19 pandemic.

While innovative modes of service delivery and increasing ease of access to the Internet and technology present new opportunities, they also present new challenges and questions, particularly related to keeping children safe both online and offline. These risks, to which the most marginalized children are the most vulnerable, include cyberbullying, peer-to-peer violence, exposure to violent or inappropriate content, and online child sexual exploitation and abuse (CSEA).

As education systems tap into the potential of ICT, it is critical that policy-makers, not only in education but in all relevant sectors, maintain and enact a strong commitment to child online protection both in and through digital learning. This requires a clear understanding of the laws, policies, frameworks and standards that are needed to ensure child protection in digital learning ecosystems. It also requires an understanding by governments, civil society organizations, education and child protection stakeholders, the private sector and international organizations of how these systems can be harnessed to improve child protection outcomes through increased awareness, shared-value partnerships and cross-sectoral cooperation at all levels.

Contents

Terms and Definitions

Age verification
A technical protection system that restricts access to certain digital content which is identified as inappropriate—whether by local laws or voluntarily by the content creator or host—for Internet users below a specified age.

Artificial intelligence
The use of computers or computer-enabled robotic systems to process information and produce outcomes in a way that is similar to how humans learn, make decisions and solve problems[1].

Bullying
“Intentional and aggressive behaviour occurring repeatedly against a victim where there is a real or perceived power imbalance, and where the victim feels vulnerable and powerless to defend himself or herself. The unwanted behaviour is hurtful: it can be physical, including hitting, kicking and the destruction of property; verbal, such as teasing, insulting and threatening; or relational, through the spreading of rumours and exclusion from a group.”[2]

Child safeguarding
Respecting and supporting every child’s right to be protected, nurtured, and free from all forms of violence, abuse, maltreatment and exploitation as outlined in the Convention on the Rights of the Child. child safeguarding, including for private sector actors, refers two actions taken to address how operations and working practices impact children’s safety and well-being.[3]

Child sexual exploitation and abuse (CSEA)
Sexual exploitation refers to any actual or attempted abuse of a position of vulnerability, differential power, or trust, for sexual purposes, perpetrated by aid workers against the children and families they serve. Sexual abuse is the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions, perpetrated by aid workers against the children and families they serve.

Classifiers
Machine learning algorithms that categorizes data into information categories, or “classes”, such as those which identify emails as “spam” or “not spam”.

Conduct risks
“Where a child behaves in a way that contributes to risky content or contact. This may include children writing or creating hateful materials about other children, inciting racism or posting or distributing sexual images, including material they have produced themselves.”[4]

Confidentiality
“Confidentiality is the process of protecting an individual’s privacy. It pertains to the treatment of information that an individual has disclosed in a relationship of trust, with the expectation that this information will not be divulged to others without permission.”[5]

Contact risks
“Where a child participates in risky communication, such as with an adult seeking inappropriate contact or soliciting a child for sexual purposes, or with individuals attempting to radicalize a child or persuade him or her to take part in unhealthy or dangerous behaviours.”[6]

Content blocking
The use of a program to block access to or the availability of certain content, such as web pages.

Content risks
“Where a child is exposed to unwelcome and inappropriate content. This can include sexual, pornographic and violent images; some forms of advertising; racist, discriminatory or hate speech material; and websites advocating unhealthy or dangerous behaviours, such as self-harm, suicide and anorexia.”[7]

Cyber-attack
An attack on a physical or information asset that occurs when a threat successfully breaches security controls. Cyber-attacks can be classified as active (which aims to alter system resources or affect their operation) or passive (which aims to use information from a system without affecting its resources), and as inside (an attack initiated by an entity inside the set security perimeter) or outside (attacks from beyond the set security perimeter initiated by an unauthorized or illegitimate user of a system, such as hackers, criminal groups, and other States).[8]

Cyberbullying "The posting or sending of electronic messages, including pictures or videos, aimed at harassing, threatening or targeting another person."[9]

De-identification of data The removal of personally identifiable information from data to protect privacy. While de-identified data may be able to be re-associated with the personally identifying information at a later point in time, anonymized data is that which has had personal identifiers permanently and completely removed.[10]

Digital citizenship "The ability to engage positively, critically and competently in the digital environment, drawing on the skills of effective communication and creation, to practice forms of social participation that are respectful of human rights and dignity through the responsible use of technology."[11]

Digital learning The use of digital technology to carry out teaching and learning activities, regardless of whether they take place in person or at a distance. Digital learning can be both online and offline.[12]

e-Inclusion Both ensuring that ICT is inclusive and using ICT to achieve wider inclusion objectives, focusing on participation of all individuals and communities in all aspects of the information society[13].

Filter bubbles a context in which an individual is only exposed to information or content that aligns with or reinforces beliefs which they already hold or their personal likes, most often created in online environments because of algorithmic filtering.

Grooming Sexual abuse that occurs when adults communicate with children with the aim of developing a sexual relationship. "Grooming takes place over time and a perpetrator often starts by building a relationship with a young person to find out about their needs and vulnerabilities."[14]

Hacking Unlawful access to a computer system[15].

Hashed blacklists of materials Hashes are unique, fixed-length strings produced by algorithms for any given piece of data (e.g., text, applications, content or pictures). Lists of these hashes can be created for any application or content which may pose a security risk or is restricted by an organization's IT policy. Then these hashes are used to block access to computer systems by these applications or content. It is a form of security by controlling the content or application's access to organization's or individual computers.

Heuristic filtering The use of high-level algorithms and programming of computers to apply specific intuitive criteria or experience (instead of technical metrics) to the analysis and filtering of content.

Learning management system (LMS) A type of software that organizes the educational process within different learning environments, allowing learners to find materials linked to the study plan, collaborate with others, submit assignments, and communicate with instructors. LMSs can, in some cases, adapt learning materials to the learner's performance. Artificial intelligence can also be applied to make LMSs adaptive or 'intelligent' to regularly adjust for learners' needs[16].

Mandated reporting The legal requirement for certain people, primarily categories of professionals (e.g., social workers, teachers), to report any suspected case of abuse or neglect of children to the relevant government authorities.

Parental controls Features or software that allow adults to monitor and restrict what children do online.

Penetration testing A method of testing the security features of an information system by attempting to circumvent or defeat them

Privacy “The ability of an individual to control the extent, timing, and circumstances of sharing themselves (physically, behaviorally, or intellectually) with others. Privacy refers to the right of individuals to limit access by others to aspects of their person that can include their thoughts and identifying information.”[17]

Safety by Design A proactive and preventative approach to minimizing online threats by anticipating, detecting and eliminating them before they occur, embedding safety into the culture and leadership of an organization, and emphasizing accountability, including by encouraging technology companies to invest in front-end risk mitigation.[18]

Spam Unsolicited junk mail sent through the abuse of electronic messaging systems[19].

Two-step verification Also known as two-factor authentication or multi-factor authentication; A method for verifying the identity of a user logging onto a system that requires two steps, such as entering both a username and password and an authentication code sent to a mobile device, for example.

Universal Design for Learning An approach to teaching and learning that designs learning content and its delivery to be accessible to all learners, no matter how they learn. It shifts the thinking away from what students are not able to do and focuses on teaching and learning in a scientifically valid way that reduces barriers to quality, inclusive learning through appropriate support, high expectations, and flexibility in how content is delivered, how students interact with it, and how they are engaged with learning.[20]

Web crawler A program or automated script which browses the World Wide Web in a methodical, automated manner, for purposes that can be either helpful (e.g., providing up-to-date data) or harmful (e.g., harvesting email addresses for spam)[21].

Zero-rating When an Internet Service Provider “applies a price of zero to the data traffic associated with a particular application or class of applications (and the data does not count towards any data cap in place on the internet access service).”[22]

Acronyms

AI	Artificial intelligence
COP	Child online protection
CSAM	Child sexual abuse materials
CSEA	Child sexual exploitation and abuse
CSOs	Civil society organizations
EMIS	Education management information system
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information communication technologies
INTERPOL	The International Criminal Police Organization – INTERPOL (“International Police”)
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
LEAs	Local education authorities
LMS	Learning management system
NGO	Non-governmental organization
SIM	Subscriber identity module
UDL	Universal Design for Learning
UNCRC	United Nations Convention on the Rights of the Child
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children’s Fund
URL	Uniform Resource Locator

© UNICEF/UNI321762/Filippov

Introduction

In 2020, UNICEF Regional Office for Europe and Central Asia significantly scaled up its work on digital learning, in line with global priorities set forth by Reimagine Education and in light of the need created by the COVID-19 pandemic and related interruption of face-to-face learning. This work is operationalized in Europe and Central Asia by the *LearnIn* and *PlayIn* initiatives. *LearnIn* is led by the UNICEF Regional Office Education Section and aims to accelerate learning outcomes for vulnerable children through effective, inclusive, equitable, technology-enhanced learning opportunities integrated with the instructional core. *PlayIn* is led by the UNICEF Regional Office Early Childhood Development Section and aims to provide digital platforms for early childhood educators and parents to support play-based learning and development for early learners. Both initiatives aim to support education systems to harness the power of technology to support the provision of quality, inclusive, personalized and flexible learning during and beyond the pandemic.

The *LearnIn* Implementation Plan (2020-2025) outlines a set of initial considerations, informed by existing UNICEF resources on child online protection in the context of COVID-19[23], the principles of Safety by Design by the e-Safety Commissioner of Australia[24] and Model National Response to online child sexual exploitation by the WeProtect Global Alliance[25]. The section was developed through consultation with colleagues across sectors, namely child protection colleagues from UNICEF HQ, and with UNICEF partners. Though brief, the inclusion of data privacy and online safety in the *LearnIn* Implementation Plan aims to serve as a signpost of the importance of these issues for all working on the design and implementation of digital learning.

As countries accelerate the development of digital learning with the support of UNICEF and in cooperation with a wide range of partners at the local, national and regional levels, however, it is imperative that countries are also supported to uphold their responsibility and commitment to keep children safe, including in digital environments. At the same time, it is important that technological innovation in education be leveraged to support children's safety and well-being. What is needed now is more than a signpost. Rather, a set of action-oriented considerations could guide governments and partners to address these challenges and tap into this potential by outlining where these needs and opportunities might exist among various actors and at all levels across digital learning ecosystems.

UNICEF is uniquely positioned to provide this support to countries in Europe and Central Asia. In May 2021, the UNICEF Regional Office for Europe and Central Asia noted in its Strategic Directions White Paper, *Advancing Child Online Protection in Europe and the Neighborhood*, that the organization's regular and consistent child protection engagement with key government and non-government stakeholders are natural entry points for supporting child online protection. UNICEF's ongoing support on digital learning and education system strengthening in Europe and Central Asia provide a critical opportunity to channel the organization's comparative advantage and harness ongoing work on child online protection in the region to embed child online protection into digital learning ecosystem development and education system digitalization. UNICEF remains committed to supporting governments to guarantee the protection and safeguarding of all children while also harnessing digital technology to safely and equitably accelerate learning and protection outcomes.

Purpose and audience

This document intends to operationalize UNICEF's commitment to support governments as they develop digital learning ecosystems that are inclusive and safe for all children. It provides a set of considerations that contextualize existing guidance on child online protection more specifically for digital learning. Its purpose is to support education decision-makers and actors in relevant sectors to prioritize child online protection in the digitalization of education systems but also to center digital learning in strategies to address child online protection risks and improve child protection outcomes, both online and offline. It is designed to encourage thinking and dialogue among stakeholders and across education lifecycle and system levels, and evidence-based planning and decision-making on child online protection as it relates to digital learning. In short, this document aims to support the integration of child online protection considerations into every component of work on digital learning. The intended audience of this document includes education decision-makers at all levels of government; their counterparts in relevant sectors such as social policy and social protection, law enforcement, justice, telecommunication, and health; UNICEF Country Offices; implementing partners; the private sector; and any other stakeholders involved in the design and implementation of digital learning.

How to use the document

UNICEF's Digital Learning Strategy for Europe and Central Asia outlines several programmatic approaches, or pillars, for supporting the development of digital learning ecosystems. These include connectivity, device access, digital learning platforms, quality content, teacher professional development and support, and children's and parents' engagement and support, as well as support to the enabling environment (i.e., systems strengthening, evidence generation, communication and advocacy, and partnerships and financing). These are operationalized through the regional *LearnIn* and *PlayIn* initiatives for digital learning for early childhood and basic education, respectively.

This document offers questions organized under key pillars for consideration when planning and developing digital learning ecosystems. While these pillars—and, thus, the sections of this document—represent parts of the whole digital learning ecosystem, they are interconnected and indivisible; it is critical that these considerations are viewed together rather than as individual checklists of tasks.

The questions posed are based on international guidance, national policies, evidence on child online protection risks and mitigation, and UNICEF's significant experience in supporting child protection efforts in Europe and Central Asia and across the world. They reflect UNICEF's ongoing support to governments to provide inclusive, quality, digitally-supported learning opportunities for all children and to prepare for and facilitate the inclusive digitalization of education systems throughout the region. However, while this document aims to summarize priorities, main risks and opportunities related to child online protection in and through digital learning, it intends to be neither authoritative, comprehensive, nor final. Stakeholders using this document should therefore also consult existing policies and legal frameworks for child protection as they apply in contexts of education and digital environments, particularly in their own countries, and should read this document keeping in mind the rapidly evolving nature of digital technologies and the need for continual revision.

Child Online Protection Risks relevant to Digital Learning

It is imperative that all involved in digital learning—from governments developing digital learning policies to private and public sector partners designing digital content and platforms—are aware of not only the opportunities, but also the risks of children's increasing engagement with digital technology so that they can proactively address them. Some of these risks include, for example, exposure to suicidal content, discrimination, online gambling, hate speech, child sexual abuse material (CSAM), sexual exploitation and trafficking. The EU Kids Online network offers a framework for understanding the risks and potential harm to children online and in digital environments by outlining commercial, aggressive, sexual, and value risks in the areas of content (child as recipient), contact (child as participant) and conduct (child as actor). For example, aggressive content risks can include a child receiving violent or hateful content, contact risks can include being bullied, harassed or stalked, and conduct risks include the child bullying or harassing others. Sexual risks include receiving harmful sexual content (content), meeting strangers or being a victim of grooming (contact), or creating or uploading pornographic material (conduct). These are shown in Table 1.

Children who are exposed to inappropriate, harmful, or criminal content may be led to extremes, including self-harm, destructive behaviour, violence, radicalization, and the development of racist or discriminatory ideas[26]. Personalization based on children's strengths, needs and interests is an opportunity presented by digital learning and the increasingly advanced capabilities of artificial intelligence (AI). However, algorithmic filtering and customization of content according to user behavior can also create echo chambers or "filter bubbles," which can prevent access to information and a variety of ideas and unintentionally limit children's development[27]. Increased access to digital technology can also blur the lines between where children experience bullying and other contact threats from peers and adults and where they are safe, with the most marginalized children, namely children with disabilities, more likely to be victimized by bullying, exclusion, harassment and, especially, sexual victimization[28]. Through technology, it is much easier for children to be targeted, abused and groomed by someone close by or across the world. As their lives, including their learning, increasingly occur in digital spaces, children also face risks regarding their own conduct which, when inappropriate or illegal, can lead to lasting consequences. For example, children may inadvertently disclose their own personal information and place themselves at greater risk online and offline, they may infringe on rights through plagiarism or uploading content without permission, they may infringe on copyright, such as by illegally downloading audio or video content, share inappropriate content with others, or spend excessive time online at the cost of their physical or mental health and well-being[29].

Often, inappropriate activities and the risks that they pose may occur because they are technically allowed by terms and conditions that have not been designed with children rights and needs at the center[30] or because of inadequate planning to address these risks. Building in protections and developing digital learning platforms, content and technology according to the principles of Safety by Design can help to prevent them. It is not enough, however, for the responsibility to lie solely with developers and users; rather, decision-makers and their partners play a key role in mitigating these risks and responding appropriately to any possible harm. In fact, it is critical that public awareness, political will, education ethos, end product design and operations all keep children safety and rights clearly in mind[31]. These issues concern government agencies, law enforcement, social service organizations, schools and non-formal education providers, Internet Service Providers (ISPs) and other Electronic Service Providers (ESPs), mobile phone network providers, public Wi-Fi providers, tech companies, parent and teacher organizations, NGOs, academia and the research community, actors who own and operate public access points and others[32], and it is important for there to be a shared understanding of what safe digital learning looks like, as well as shared commitment to achieving it.

Table 1. A Classification of online opportunities and risks for children

		Content: Child as recipient	Contact: Child as participant	Conduct: Child as actor
Opportunities	**Education learning and digital literacy**	Educational resources	Contact with others who share one's interests	Self-initiated or collaborative learning
	Participation and civic engagement	Global information	Exchange among interest groups	Concrete forms of civic engagement
	Creativity and self-expression	Diversity of resources	Being invited/ inspired to create or participate	User-generated content creation
	Identity and social connection	Advice (personal/ health/ sexual, etc.)	Social networking, shared experiences with others	Expression of identity
Risks	**Commercial**	Advertising, spam, sponsorship	Tracking/harvesting personal information	Gambling, illegal downloads, hacking
	Aggressive	Violent/ gruesome/ hateful content	Being bullied, harassed or stalked	Bullying or harassing another
	Sexual	Pornographic/ harmful sexual content	Meeting strangers, being groomed	Creating/ uploading pornographic material
	Values	Racist, biased info/ advice (e.g., drugs)	Self-harm, unwelcome persuasion	Providing advice, e.g., suicide/pro-anorexia

Source: Livingstone & Haddon, 2009[33]

Considerations

1. Enabling environment

This section introduces child online protection considerations related to the enabling environment supporting digital learning ecosystems. It covers the themes of awareness, preparedness and political will; functions, legislation, policies and frameworks; and partner engagement and commitment. Adequate focus in the enabling environment that support digital learning ecosystems should be given to translating political will into concrete action. Strategies and policies, for example, must be implemented in practice and supported with the appropriate budget.

1.1 Awareness, preparedness and political will

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do policymakers, legislators, and senior-level decision-makers across sectors, including education, recognize child sexual abuse and exploitation, cyber-bullying, violation of data privacy and other online risks as problems which leaders must address and risks that must be mitigated in digital learning and the digital transformation of the education sector?	●		●		●					●		
Do governors, municipal leaders and other local level leadership recognize child sexual abuse and exploitation, cyber-bullying, violation of data privacy and other online risks as problems which leaders must address and risks that must be mitigated in digital learning and the digital transformation of the education sector?							●			●		
Is adequate attention given to safeguarding children's rights in the digital environment (not limited only to data privacy and security) and are child online protection risks identified, mitigated and responded to appropriately?	●		●		●		●	●		●		

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Have policymakers and legislators set clear objectives for identifying, mitigating and responding to child online protection risks in and through digital learning across the whole learning continuum? Are regulations by relevant national and local authorities, including but not limited to national and local education and ICT authorities, aligned with these objectives?	●		●		●		●	●				
How are recognition of the importance of child online protection and commitment to these issues maintained if and when transitions in leadership take place? For example, do these issues receive adequate and sustained attention across relevant strategic, development, and annual plans?	●		●		●		●	●		●		
Are adequate government resources (human and financial)available and allocated for addressing child protection risks in digital learning? Are adequate government resources available and allocated to support education systems to build the necessary processes and mechanisms for identifying and mitigating child online protection risks into digital learning systems?	●		●		●		●	●		●		
Is the current political will enough to ensure long-term commitment to and resource availability for child online protection, including across changing administrations and political cycles? For example, is there a commissioner or national rapporteur whose role includes specific focus on child online protection in digital learning?	●		●		●		●	●				
Does political leadership at the national and local levels, and especially do the national (or regional) Ministry of Education and local education authorities demonstrate efforts to shift harmful social norms that may perpetuate child online protection risks, including but not limited to child sexual abuse and exploitation?	●		●		●		●	●		●		●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Have national and local efforts to raise awareness of child online protection focused on risks in digital learning and targeted education and telecommunications authorities, schools, education administration, education personnel, children, parents, and community organizations? Have they also specifically targeted the private sector?	●		●					●	●	●	●	●
Do policymakers participate in international networks and conversations to ensure that policy deliberations on child online protection are informed by the growing international knowledge base?	●											
Have all actors, particularly education actors, policy makers, and law enforcement, been trained on issues of child online protection?	●	●	●		●	●	●	●	●	●	●	●
Have dedicated training and professional development for policy leaders, law enforcement and judicial functionaries been offered on child online protection (CSEA?) and have these capacity strengthening efforts included explicit attention to the implications for the delivery of services, namely education, and the needs of the education sector?	●	●	●		●	●	●	●		●		
Have child protection professionals and mental health providers received training, resources and support to ensure they are aware of and ready to support on child online protection issues including specifically as they relate to digital learning?	●						●			●		
Do school leaders understand (and have they received capacity strengthening support to carry out) their responsibility to oversee the safe use of digital technology when learners are in their care and to take timely and appropriate action when any concern about risk to online safety arises? Have they been supported to ensure that they understand how and to what extent this responsibility extends also when learners are not physically present in schools but are engaging in education delivered virtually or at a distance?[34]		●	●			●		●	●	●		

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do national or international self-assessment tools for school and education system readiness for digital learning adequately consider the presence of, familiarity with, and needs related to child online protection laws, policies and procedures?	●		●			●				●		

1.2 Functions, legislation, policies and frameworks

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
General												
Has a national framework, which outlines principles for child online protection and priorities for action and collaboration, been developed with a wide range of actors and adopted?	●		●		●					●		
Does a specific function (such as an eSafety Commissioner) exist at the national level, either as an independent regulatory agency or within another ministry such as ICT, to address child online protection risks? Do they collaborate with and receive support from other relevant actors, including national and/or local ministry(ies) of education, ICT or telecommunications ministries, schools, NGOs, and the private sector?	●		●		●		●	●	●	●	●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
If a specific function (such as an eSafety Commissioner) exists to address child online protection risks, do they have the power to administer services to mitigate and address such risks, such as complaint mechanisms for children whose right to be protected online has been violated, and the power to investigate and address such complaints, such as by requiring the removal of material identified as harmful to children[35]? Are schools aware of this function and supportive of its role?	●		●		●		●	●	●	●		●
Are arrangements in place to enable such a function or body, as well as other public and private actors (e.g., through law enforcement cooperating with INTERPOL, or through specialized hotlines/helplines) to exercise rapid content-blocking power in the event of online crises or cyber-attacks to prevent exposure, particularly of children, to extremely harmful material?	●											
Are functions and responsibilities of national and local authorities in running educational programs for online safety clearly established and delineated, and is the role of education authorities in ensuring that these programs reach school communities clearly outlined?	●		●					●	●			
What policies are in place to ensure the age- and developmentally-appropriate and supervised use of digital devices for learning, especially during periods of distance learning when children might be home alone?	●						●					

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
What laws and policies govern the interaction that teachers, schools, and education systems are able to have with children and their families via technology that was not intended specifically for educational purposes? For example, are teachers allowed to reach out via social media or messaging applications to children who are not participating in or cannot access digital learning platforms? Are schools allowed to use social media to deliver learning content or information to children who have dropped out or children on the move when other means do not reach them? If so, how is learners' protection guaranteed in these interactions?	●		●						●			
Is there a national code, framework or set of standards available to schools that establishes clear rules for online behaviour among education staff and children across the learning continuum? For example, is it recommended that staff, personnel and volunteers not accept connection requests on personal social media accounts from their students and families[36]?			●			●		●	●			
Has law enforcement established clear mechanisms for reporting incidents or concerns through collaboration with other key actors, including in education and child protection? Have policy-makers worked together with law-enforcement and other stakeholders to ensure open but safe communication channels?[37]	●	●	●				●					
Does the system count on specialized agencies or stakeholders with the specific mandate to support child online protection at the local level? If so, have they been engaged with schools and local education authorities to ensure close collaboration on these issues? Have they been involved in the development and implementation of national legal, regulatory and policy frameworks on child online protection?[38]	●	●					●	●	●			

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Has a stakeholder analysis and/or mapping been conducted to support clarification of the roles, responsibilities, interests, and potential areas of collaboration of various actors that spans all stages of the development of digital learning ecosystems, all levels from national to local and both the public and private sectors?	●		●									
Has your country engaged with other countries in your region and beyond in efforts to harmonize your legal frameworks and to support international cooperation to protect children online?	●	●										
Is the definition of "child" standardized in all legal documents, frameworks, and procedures as anyone under the age of 18? Are all actors strictly held to this definition, including in virtual environments? For example, are private sector actors, including those who provide educational technology tools or services, prohibited from treating any children who might be under the age of 18 but old enough to consent to data processing as an adult?	●	●	●		●						●	
Does legislation exist to define and legislate against child abuse and exploitation, including online, grounded in the United Nations Convention on the Rights of the Child?	●											
Does legislation that covers child online protection address prevention, intervention and response for child sexual exploitation and abuse?	●	●	●		●		●	●				
Is terminology consistent across legislation regarding the definition of child online protection risks, and reporting, identification and removal of harmful content?	●		●	●	●							
Do policies exist to specify basic online safety expectations, including for all education actors? Have these policies been developed or revisited alongside advances in the national and/or local digital learning ecosystem?	●		●		●							

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are terminology, definitions, and thresholds consistent among child protection legislation and education policies, including for digital learning? Do terminology, definitions and thresholds applied in digital learning support national efforts to hold both the public and private sector accountable for ensuring children's rights to both protection from violence, exploitation and abuse and to education?	●		●									
Have legislation and policies been developed to address threats from outside of the country, especially as learning content may include international resources? Is there a flexible, up-to-date, cross-country model or system in place for criminal justice collaboration that includes prevention, intervention and response to child protection risks in digital learning?	●	●	●									
Are versions of policies and laws related to child online protection available in child-friendly and parent-friendly language and communicated with schools, communities, and organizations that represent parents and children?	●		●					●	●	●		●
Do policies on child online protection, including those that address digital learning, acknowledge that the internet and related tools and services reproduce and reinforce offline practices and thus view child protection online and offline as mutually influential rather than isolated worlds[39]? With this in mind, do they account for how the risks children face online might influence their safety, well-being, and learning offline?	●		●	●	●							
Do child protection laws, policies and legal frameworks from relevant sectors (including social protection, social policy, law enforcement, justice, and telecommunications) explicitly address their application in digital environments, specifically digital learning environments?	●		●	●	●							

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Has a thorough analysis been conducted to identify any gaps in national legal frameworks and policies between what is illegal offline and what is illegal online? Is this analysis grounded in the understanding that any crime that can be committed against children offline can, mutatis mutandis, be committed online[40]? Has this analysis considered specifically online learning environments and the use of digital technology for education delivery and learning?	●					●						
Does legislation establish that there are no spaces (especially digital learning platforms and other education-related digital environments) that are outside of child protection law and that any crime that can be committed against children offline can, mutatis mutandis, be committed online[41]? Has the education sector been included in efforts to provide harmonized standards for adjudicating and investigating cybercrimes in both substantive and procedural law?	●		●	●								
Have existing practical instruments, including from the education sector, from other countries and from organizations such as ITU, been consulted in the development of a cybersecurity legal framework and related laws?	●											
Is there a process in place for transferring unsafe material to law enforcement if it has been seized by other actors, such as schools? Is there a process in place for examining material seized by law enforcement and other actors to establish whether victims are identifiable and to assess other harms and risks to which they may have been exposed?[42]	●	●	●	●	●		●		●			
Do policies on child online protection grant the appropriate authorities the power to investigate complaints about dangerous and/or violent (including serious cyberbullying) material targeted at children, including when this material is shared via services or on platforms used for educational purposes?	●	●	●		●		●	●	●			

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do child online protection policies include clauses that grant the appropriate authorities, bodies or functions (such as an eSafety Commissioner) the power to request or require internet service providers to disable access to any learning material, platform or service that depicts, promotes, or incites violent, abusive or unsafe conduct in extreme situations?	●	●	●		●		●	●	●			
Sometimes, internal remedial and grievance mechanisms, such as those established by businesses providing the digital learning platform, tool or content, may prove ineffective in providing remedies in cases deemed harmful to children. For example, cyberbullying content may be deemed harmful but remain unaddressed by national legislation; therefore, the content host may not seek the removal of such content. In cases such as this, is there a public authority that is able to receive such complaints, cooperate with relevant actors (such as education stakeholders), and intercede with the content host to remove the content?[43]	●	●	●		●		●	●	●		●	●
Beyond removal notices, are there mechanisms in place for holding service and content providers accountable for the safety of their services and content for learners?	●	●	●		●					●	●	●
Do laws establish mandated reporting by certain professions, including those in education, and do these laws also cover interactions that such professionals may have with children in virtual environments, such as in digital learning? Are policies in place to guide mandated reporters and have these policies been updated to accommodate digital learning? What protections, including anonymity, are in place for reporters, particularly if reporters are children?	●	●	●	●		●			●			
Does the law oblige education authorities, schools, administrators, teachers, and content providers to cooperate with criminal justice functionaries? How are such obligations expanded to include instances when there are concerns of children's safety in digital and distance learning?	●	●	●					●	●			

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Is there a legal framework that governs all education-related actors (including the private sector) and lays out how local education authorities, schools, administrators and education personnel are involved in and/or related to processes of reviewing, reporting, responding to and investigating reports?[44]	●		●					●	●			
Does the country have a universal content classification system to facilitate data sharing on child online safety?[45]	●			●	●							
How are measures to protect children online balanced with other rights such as freedom of expression and the right to access information for learning, especially within spaces facilitated by adults, such as digital learning environments?	●		●									
Are policies in place that outline the type of support available to victims of online abuse, including the channels for seeking it and the delivery of this support? Do these address the types of support available to children and their families, and is special consideration given to how this support is provided when they have been victims in online learning environments? (E.g., are services that might most often be offered through the school offered via other channels if the child was abused by teachers or encountered harmful learning content on the national learning platform?)	●		●									
Do child protection laws institutionalize the use of official referral pathways that enable qualified professionals across sectors, including education professionals, to connect victims and their families with locally available, professional services? Are accommodations made for situations in which face-to-face assessments or service delivery may not be possible (e.g., in distance learning) to ensure that timely referral and support are provided?	●		●	●			●	●	●	●		
Has the country developed a national response to online child sexual exploitation, guided by the Model National Response[46]?	●	●	●	●	●	●	●	●	●	●	●	●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Does policy and legislation facilitate transparency and enable education actors to easily access information regarding how and the extent to which private sector partners (such as providers of content, platforms and other services to support digital learning) support child online protection? Are there specific policies and norms in place to support public sectors (including education) to prioritize child online protection in their partnerships and interactions with the private sector?	●		●								●	
Education policy and planning												
If a child online protection strategy exists, is it fully integrated with existing policy frameworks related to education?	●		●	●								
Has the education sector included child online protection considerations, predicated on the UNCRC, when integrating digital learning into existing education legislation?	●		●	●								
Do Education laws, policies, statutory guidance address child online protection? In what way do these laws acknowledge and address the risks of digital learning?			●									
Do Education strategies and plans that relate to digital learning consider the risks to child protection that digital learning environments present? Do they consider the opportunities that digital learning environments provide to strengthen child protection processes and improve child protection outcomes?			●					●				
Does education legislation include or make reference to a clear set of norms or behaviours for online learning and digital communication, including regulations for the reporting of child online protection concerns?[47]	●		●									
Have education sector analyses, needs analyses and other assessments used to determine priorities in digital learning assessed child online protection risks that children face in digital learning environments?	●		●									

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are there education policies in place that explicitly protect victims of child online sexual exploitation and abuse, radicalization, or other child protection abuses from exposure and/or punishment by education actors (such as teachers removing a child's "privileges" related to digital technology use in the classroom)?	●		●						●			●
Do education policies and strategies address e-inclusion (e-Inclusion means both inclusive ICT and the use of ICT to achieve wider inclusion objectives. It focuses on participation of all individuals and communities in all aspects of the information society), and especially the diverse and increased risks that vulnerable groups may face in online learning more than others?[48]	●		●									●
Do education policies reflect industry standards for self-regulation (including the codes of conduct and institutional practices involved in content classification, age verification, data protection and the treatment of personal information) in relation to digital platforms, tools, services and content for educational purposes[49]? Have they considered whether industry standards are adequate when it comes to protecting learners?	●		●								●	
Are there national standards for child online protection, including for preventing and responding to child rights violations, that are applied by Education authorities as conditions for businesses (including technology providers) to qualify for funding or contracts? Are companies and organizations provided supporting documents for developing safeguarding policies and child protection procedures?[50]	●		●					●			●	
Do technical assistance guides, written in collaboration among child protection and education authorities and leading experts on online protection, exist to support education actors with comprehensive, safe digital learning planning efforts?			●	●	●	●						

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are referral pathways that enable education professionals to connect victims and their families with locally available, professional services formally recognized in education policies? Do policies clearly outline a process for utilizing such pathways and engaging such services, for all forms of risk that children might encounter online (e.g., sexual abuse, radicalization)? How are these policies and processes enforced?	●		●	●								
Are support, accommodations, and alternative learning arrangements guaranteed for children who have been victims of child online sexual exploitation, abuse, or other harms? How is the availability of such arrangements made known to victims, their parents and caregivers, and teachers to ensure continuity in education service delivery? What policies are in place to ensure timely requests for and delivery of such arrangements and support? Who is responsible and accountable and how is this enforced? How is the quality of such alternative arrangements monitored?	●		●	●			●	●	●	●		●
Do education provisions and support for particularly vulnerable groups of children, namely children with disabilities and migrant or refugee children, include specific attention to keeping them safe in online learning environments or when digital tools and platforms are used to support education delivery? Do individualized education plans for children with disabilities, for example, specifically note what support might be needed for them or their families to ensure that they can not only access digital learning but also do so safely? Do supports focused on the orientation or integration of refugee and migrant children into formal education systems include attention to the support that might be needed when education is delivered digitally?	●		●				●	●	●			

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Content												
What obligations do companies have regarding the detecting, blocking and removal of harmful content from platforms and services? What obligations do companies have to provide clear reporting routes and access to support?[51]	●		●		●						●	
Do policies on child online protection establish online content schemes for the removal of certain material? Do they include complaints-based removal systems that can be accessed by learners, teachers, parents, and school administrators? Are there clear instructions and accessible pathways for using these channels/ reporting mechanisms?	●		●		●			●	●			●
Do policies outline multiple classes of materials that are considered unsafe, inappropriate and harmful and establish when authorities responsible for monitoring material and responding to complaints must notify law enforcement? Do these policies consider the role of teachers, education administrators, and service providers in these processes?	●	●		●	●				●			
Do policies oblige companies, especially those developing educational content, platforms, tools and other resources, to have and use mechanisms for detecting, blocking and removing harmful content from these resources, as well as for providing reporting routes and access to support?[52]	●										●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Digital skills												
Do education policies, standards and curricula prioritize the development of responsible digital engagement knowledge and behaviour and critical digital literacy skills for learners at all levels of education, including at the pre-primary in developmentally appropriate ways? Are these skills taught from a rights-based perspective and do they focus on skills and competencies, as well as social and emotional learning for healthy relationship building online and offline? Do frameworks for these skills cover the following areas: digital identity, digital use, digital safety, digital security, digital emotional intelligence, digital communication, digital literacy and digital rights[53]? Are they integrated across curricular subjects rather than as episodic modules or workshops?	●		●			●		●	●			
Do policies, standards, competency frameworks and curricula for teacher education prioritize teachers' responsible digital engagement, critical digital literacy, the skills needed to keep children safe online and the pedagogical skills needed to support children's development of these skills in the above areas?	●		●			●						
Platforms												
Are there age-appropriate or child-friendly and safe design codes for the development of digital platforms and the delivery of online services? Are these acknowledged in national legal frameworks?	●		●		●						●	
Are child risk assessments and safety reviews established as a prerequisite for any educational platforms and content targeting children, especially those considered for formal education delivery? Are minimum thresholds and standards established against which the results of these assessments and reviews can be compared? Who is responsible and accountable for this process?	●		●		●							

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do laws require child risk assessments and safety reviews to be conducted on educational platforms and digital learning content intended for children before implementation? Do policies provide guidance on how child risk assessments and safety reviews should be conducted regarding educational platforms and content targeting children?	●		●									
Are there laws or policies in place that prohibit the use of digital learning platforms for advertising?	●										●	
What laws, policies, and disciplinary procedures are in place to prevent the selling of children's data gathered from digital learning platforms and their use of other educational tools and resources?	●	●									●	
Does the concept of cyber-bullying—and policies to prevent and respond to it—encompass all platforms and services where children might interact beyond social media, such as digital learning platforms, discussion boards, videoconferencing and other tools, services and platforms that children (and teachers) used for learning purposes?	●		●									
Does the criminalization of grooming extend also to cases where sexual abuse occurs via virtual meetings, such as on or through digital learning platforms?	●	●	●	●								
Responsibilities and accountabilities												
Is there a clear delineation of responsibilities and accountabilities related to child online protection in digital learning among education actors at the various levels of the education system? What systems are in place to ensure that all actors aware of these responsibilities and what they entail? How are they held accountable? To what extent are local education authorities (LEAs) and schools autonomous in relation to digital learning and how does this impact considerations for child online protection?	●		●			●		●	●	●		●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Does a functional cross-sectoral coordination body for child online protection exist at national and sub-national levels?	●	●	●	●	●	●	●	●	●	●	●	●
Is there a clear delineation of responsibilities and accountabilities related to child online protection in digital learning among education sector partners, including other sectors (e.g., Justice, Social Affairs) and the private sector?	●	●	●	●	●	●	●	●	●	●	●	●
Integration, reporting and continuous development												
Has an approach been taken that not only develops specific legislation to govern digital environments, including digital learning environments and digital education delivery, but that also integrates key considerations related to education delivery via digital means into existing legislation?	●		●	●	●							
Are laws and policies developed with the understanding that children are not a homogeneous group and that responses might need to be differentiated according to children's age, developmental level, specific needs, and/or additional vulnerabilities and heightened risk[54]? Are provisions made to ensure that such responses are based on a thorough understanding of a child's unique developmental level and needs, such as through consultation with a wide range of actors who would be familiar with these, including parents and the child, teachers, medical professionals, wraparound services, and others?												
Do policies establish responsibilities and mechanisms for collecting data on and monitoring child online safety? Is the role of schools, education authorities, and education personnel in supporting efforts to monitor online safety clearly defined?	●		●	●				●	●			
Are there strategies and mechanisms in place to enable the efficient and effective sharing of information, both among education authorities at different levels of the system and among authorities in education, social affairs, justice, and other relevant sectors?	●		●	●	●		●	●	●	●	●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Is data on child online safety used together with education management information system (EMIS) data for informed decision-making on online learning?												
Does the collection of child data, learning data and data related to child online safety comply with General Data Protection Regulation (GDPR) or relevant national data protection laws?	●		●		●							
Have the risks associated with collecting information on child online safety been identified and mitigated? What legal measures have been enacted for ensuring that information on child safety is accurate, contextualized, and de-identified? Have all personnel working with this information in any way been trained on both child safeguarding and data protection?	●	●	●	●	●	●	●	●	●	●	●	●
Are education laws and policies to keep children safe in online learning conceived specifically enough to provide clear guidance? At the same time, are they conceived broadly enough to be responsive to and inclusive of ongoing or future technological development and the rapidly changing landscape of digital technologies (e.g., artificial intelligence), their use for learning, and children's changing practice? Are they technology neutral to ensure that their "applicability is not eroded by future technical developments"[55]?	●		●	●	●							
What legal and regulatory frameworks exist to govern areas of ongoing and future technological development, such as the use of artificial intelligence for educational purposes or other innovation that might not yet fall under existing child protection frameworks?	●		●	●	●							
Is there a self- or co-regulatory policy or framework that includes codes, best practices and minimum standards, both for multistakeholder engagement and coordination and for formulating and enacting responses to technological change?[56] What penalties, if any, exist for policy infringement?	●											

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
If a child online protection strategy exists, is it fully integrated with existing policy frameworks related to education?	●		●	●				●				

1.3 Partner engagement and commitment

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do policymakers, national and local authorities engage their partners, the private sector, and all education actors and stakeholders at the national, district and local level on the importance of child online protection? Does this include those stakeholders who are the most marginalized (e.g., refugee children, families living in remote areas, students with disabilities, out-of-school youth accessing education through non-formal, digital pathways, etc.)?	●		●		●	●	●	●	●	●	●	●
Are all education actors and stakeholders at the national, district and local level, included in decision-making related to keeping children safe online and in setting related priorities?	●		●		●	●	●	●	●			●
Do private sector partners with whom the government works on issues related to digital learning include child online protection among their priorities?	●		●		●						●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Is there cooperation between the Ministry of Education and counterparts in Ministries of Social Affairs, Justice, and other relevant ministries to determine risks, priorities and opportunities in keeping children safe in and through online learning?	●		●	●	●							
Are there policies and procedures in place that enable other sectors, such as social and mental health services, to leverage digital learning platforms to connect with children who are victims of abuse or exploitation?	●		●	●								
Do policymakers work closely with specialists in the domain of empirical research on child online protection? Do they prioritize the identification, evaluation and interpretation of available evidence, including from beyond their national borders and with a focus on evidence from multiple sectors, including education?[57]	●					●						
To what extent have education stakeholders (including education decision-makers, administrators, teachers, parents/caregivers and children) been consulted on the development of child protection laws, policies and legal frameworks around child online protection in digital learning?												
Do partners such as NGOs, UNICEF, and other organizations with whom the government works on issues related to digital learning include child online protection among their priorities?	●		●		●					●		

2. Financing and partnerships

This section presents considerations for financing for digital learning and the development and strengthening of partnerships, both with the public and private sector, to support the delivery of digital learning.

2.1 Financing

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Have the costs of keeping children safe in digital learning been assessed and financing exercises updated accordingly? Have these costs been incorporated into education funding formulas?	●		●	●	●	●						
What are the additional costs associated with keeping children safe in digital learning environments, such as the cost of digitizing reporting mechanisms and resources and training teachers and school staff? Which budgets are responsible for these costs, and, if education, do education budgets allocate for digital learning include these costs?	●		●	●		●		●	●			
Are sufficient human, technical and financial resources made available for the relevant education actors to effectively carry out their roles and responsibilities related to the national child online protection strategy and coordinating framework? Who is responsible for these costs and how is this formalized?			●					●	●	●		●
Do policies and plans address who is responsible for the costs associated with the identification and removal of harmful material from digital learning platforms, education-related sites, or any other platform or tool used for or to support the delivery of formal (and non-formal) education services?	●		●					●		●		

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Which sector is responsible for the costs associated with aligning and connecting digital learning systems and processes with the national child protection system and child protection services? Have these costs been reflected in the appropriate sector budgets and adequate funding allocated to ensure the related actions and responsibilities are carried out?	●		●	●			●	●				
Do digital learning initiatives and projects funded by partners include budgets specifically for child protection considerations?			●									
How are the costs of digital learning on families counteracted to ensure that digital education delivery does not contribute to growing inequity and further marginalization of vulnerable children? For example, if migrant and refugee children are purchasing pre-paid phone cards to access digital learning, to what offline protection risks might this make them increasingly vulnerable, and how are these mitigated?	●		●	●			●	●	●	●		
What financial resources are available for the use of both offline and online channels, such as digital learning platforms, to deliver specialized support, such as counselling, for victims who have been exposed to harm or abuse in or outside of the context of digital learning?	●		●	●								

2.2 Partnerships

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are risks and responsibilities related to child online protection in digital learning included in all agreements made with private sector partners? Are partners responsible for reporting on child online protection risks, mitigation measures, and outcomes (including incidents)?			●							●	●	
Are there existing partnerships or plans in place to seek partnerships to increase available resources for child online protection in digital learning?			●							●		
Have key stakeholders been engaged through CSOs and youth/adolescent organizations and been consulted on their priorities, insights, needs and concerns related to COP in digital learning?			●	●			●	●	●	●		●
Have education, justice, internal affairs, digital/information, and other relevant ministries been engaged in partnerships with independent human rights institutions and organizations on the issue of child online protection? Have these partnerships explored how these organizations can support in the following ways: implementation of international human rights standards at the national level; evidence generation on the impact of law, policies and practices on children's online protection; expertise on children's rights in court; advocacy, social and behavioral change and the promotion of public awareness and positive behaviours to support child online protection; the engagement, meaningful participation and empowerment of children and young people on these issues; and capacity strengthening on child online protection across various levels in multiple sectors?[58]	●	●	●	●	●					●		
Have teacher unions and other professional organizations been consulted on their priorities, insights, needs and concerns related to COP in digital learning?			●	●								●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Have academia been engaged in assessing risks and mitigation measures for child online protection in digital learning? Are policy makers engaged in communication with researchers to ensure that the policy agenda is accessible to and, in part, contributes to the research agenda? Does this collaboration help to ensure that the research agenda fills critical gaps in the evidence needed by decision-makers? Is the research agenda, still, however, in part independent of policy and draws more widely on existing and emerging knowledge on children's lives, education systems, society, parenting and policy? Have academics and scholars been engaged in the development of evidence-based strategies for child online protection in digital learning?[59]	●		●	●		●				●		
How is industry being engaged to promote the prioritization of Safety by Design in innovation and the development of new technology for education? How is industry being engaged as a key partner in promoting societal awareness of child online protection, especially in educational technology?	●	●	●	●							●	
Are schools and local education authorities encouraged to develop strong, community-based partnerships with civil society organizations, faith-based organizations, businesses, law enforcement agencies, parent and student councils, parent-teacher associations, and other local partners on issues related to school safety, understanding that this encompasses also child online safety?		●	●				●	●	●	●		●
In the case that partners and not the Ministry of Education are providing and/or administering digital learning platforms and content, which policies and procedures are in place to ensure compliance of these tools and materials with national child protection laws and regulations? Are all partners aware of who is responsible for monitoring and reporting on this compliance?	●		●	●							●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
What resources—including documents, platforms, repositories, working groups, or fora— are available that encourage and support private sector actors (e.g., businesses, technology providers), civil society and governments to co-develop, share, and exchange tools, resources, knowledge, and practices?[60]		●	●	●	●	●		●	●	●	●	
Have widespread communication and advocacy campaigns been organized to raise awareness on digital citizenship, safe online behaviours, child online protection and responsibilities of various actors, targeting not only parents/caregivers and children but also the private sector?			●	●	●					●	●	
How does the government ensure accuracy and neutrality of information developed and/or disseminated by private sector partners as part of campaigns to address child online protection and awareness raising among children and their families?	●		●	●	●							
Is the media aware of, trained on, and consistent in their use of terminology for reporting on child online protection issues, including in digital learning?[61] Are they trained in rights-based approaches for reporting on child protection and digital/online learning issues?				●						●	●	
Are all partners, including businesses who might be engaged with education delivery through arrangements such as mentorships, internships, apprenticeships or other on-the-job training, including in digital or virtual environments, required to be trained on responsible digital engagement, online safety, digital citizenship and child protection issues? How is this enforced and monitored?	●		●	●				●	●	●	●	
Are all partners, including individuals from the private sector who may be engaged in digitally-administered mentoring, internships or practical training with the education sector, required to have passed background checks?	●		●					●	●		●	

3. Evidence generation

This section discusses considerations for child online protection when collecting, analyzing, interpreting, and using data about children, learning—particularly on digital learning platforms—and their online risks and protection needs.

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Does data collected from digital learning platforms include types, frequency, and severity of child online safety risks, as well as other factors, such as the demographic profiles of children most at risk and common perpetrator tactics?			●			●		●				
Are a consistent set of metrics available to stakeholders for monitoring and assessing child online protection? Do they contribute to a measurable set of indicators established according to evidence-based logic models or theories of change?			●	●		●		●				
Are data validation measures in place? Are data collected, analysed and used in a regular, timely and accurate manner? Are these data integrated into existing data collection cycles and processes? What national and international expertise has been consulted in the development of these methodologies?			●	●		●						
Are the indicators, metrics and methodologies inclusive and representative, particularly of vulnerable groups such as children with disabilities?			●	●		●		●		●		●
Has baseline data been collected to allow the analysis of trends over time, and is this data analyzed regularly and timely to enable evidence-based action according to trends?			●	●				●				
Is penetration testing conducted regularly on digital learning platforms and content and are the results considered in terms of risk to child protection? Are vulnerabilities in the digital learning system identified and addressed in a timely and effective way?			●		●			●			●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are these and other risks and incidents related to child online protection included in regular assessment of the safety, scalability, and sustainability of digital learning platforms and the evaluation of digital learning programming? Are such assessments conducted and supported cross-sectorally, including in cooperation with technology engineers, education and child protection experts, criminal justice authorities, and other relevant stakeholders?		●	●	●	●	●		●		●	●	
Do such assessments centre the voices of children, youth, and their parents and caretakers to ensure that their concerns are adequately considered and addressed and their ideas included? Do the assessments include a wide range of national actors and stakeholders related to education and child online protection to include their opinions, experiences, perspectives, identified needs, and opportunities?			●	●		●				●		●
Have assessments been conducted to anticipate, identify and mitigate risks to which certain groups of children may be particularly vulnerable? Have these risk and vulnerability assessments considered age, location, gender, disability, legal status, ethnicity, language spoken at home, socioeconomic status, and other factors as well as the intersection of these?[62]		●	●	●	●	●		●		●	●	
Are these assessments and analyses included in the reports to education authorities, implementing partners, funders, and other stakeholders involved in digital learning and education service provision more broadly? Are reports and lessons learned available as public goods?			●	●		●		●		●	●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do regulators have independent access to data from digital learning platforms that could support assessments of the effectiveness of such platforms in responding to child online protection issues?			●	●				●				
Are assessments and analyses used for evidence-based decision-making related to the scale up of digital learning platforms and interventions?			●					●				
Are these assessments and analyses used to inform the development and improvement of response mechanisms and processes, capacity strengthening, and interventions?	●	●	●	●	●	●	●	●	●	●	●	
Are processes for identifying, reporting and responding to child online protection risks in digital learning monitored, assessed, and evaluated?		●	●	●	●		●	●	●			
How are these findings reported and shared with education stakeholders?		●	●	●	●		●	●		●		
How are the lessons learned from such findings used to improve the safety and inclusiveness of digital learning platforms? Is research conducted on the effectiveness of tools, processes, interventions and innovation aimed at addressing such risks?			●	●	●		●			●	●	
Are the lessons learned about the types of risks and contexts surrounding them from these assessments used to regularly develop and update educational materials on child online protection designed for teachers, parents and children?			●	●		●		●				
How is teachers', parents'/caregivers', and children's knowledge about child online protection monitored to enable more effective, targeted educational and awareness-raising efforts?			●			●			●	●		

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Have the risks or potential harm to children associated with collecting information on child online safety been identified and mitigated? Have measures been enacted for ensuring that information on child safety is accurate, contextualized through cooperation with relevant education actors, de-identified, securely stored, and adheres to legislation on confidentiality and privacy?[63] Have all personnel working with this data been trained on both child safeguarding and data protection?	●		●	●	●	●		●	●	●	●	
Are users of digital learning platforms informed of how their data is used and the steps taken to keep it safe?			●					●	●	●	●	

4. Platforms and content

This section discusses child online protection in digital learning related to the development and use of digital learning platforms and digital learning content. It considers not only how children can be kept safe on digital learning platforms and when interacting with digital content , but also how digital learning platforms and content can be leveraged to contribute to keeping children safe both online and offline. it addresses the design, development, and deployment of platforms and content , as well as resources and protection through digital learning.

4.1 Design, development and deployment

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Is a Safety by Design[64] approach enacted into all phases of development and deployment of digital learning platforms and other digital learning tools?			●					●		●	●	
Have child risk assessments and safety reviews been conducted on all digital learning platforms used for or to support the delivery of formal education services? Have such assessments and reviews been conducted on all digital learning tools and materials targeting children, including outside of formal education delivery?			●					●		●	●	
If content is co-created or crowd-sourced, what measures are in place to review material before it is published and to monitor any edits made to material intended for learners, teachers or families?			●					●		●		
Do all teachers, school administrators, education personnel working on the development and delivery of digital learning, parents and caregivers, and children have access to mechanisms for filing complaints about harmful and offensive content, and are mechanisms in place to ensure timely redress of such complaints?	●		●	●			●	●	●	●		

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are digital learning platforms equipped with additional blocking features that enable education actors such as the national Ministry of Education or schools to prevent specific content from being delivered or accessed via the platform?	●		●					●	●	●	●	
What other safety features are available or enabled on digital learning platforms, such as age and two-step identify verification (such as with unique email addresses issued by and traceable to the MoE), heuristic filtering, automated detection through classifiers and hashed blacklists of materials, web crawlers, and facial recognition of victims and perpetrators? Are any and all AI tools used for child online protection combined with additional safeguards and protocols to ensure accuracy?[1]			●					●			●	●
Are the safety features appropriate and adequate for safeguarding children with disabilities? How is this assessed and monitored?			●					●			●	●
Do all products, services and apps used for digital learning provide child-friendly terms and conditions in languages children speak at home and in multiple modes? How are the companies providing these products, services and apps prohibited from asking children to consent to things that they are not able to understand or that are not "in the best interests of the child"?[65]			●					●	●	●	●	●
What parental controls and filters are enabled on such platforms and in relation to digital learning content?			●					●	●	●	●	●

[1] A note of caution is necessary regarding AI tools for children online protection. According to the Broadband Commission for Sustainable Development (2019), academics warn that many algorithms may have biases built into them, which may mislead those who use the insights to see a relationship between two phenomena which may not exist. For more information, see https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
In addition to unsafe content, children may encounter content that is inaccurate or incomplete. What processes are in place for education actors to identify this content and improve or remove it?			●					●	●	●	●	
What processes are in place for the responsible actors to review and test from a safety standpoint all content that is developed and made available for digital/online learning?			●					●	●			
What processes is industry required to take to integrate tools that can prevent digital learning platforms from being exploited[66], such as IWF Services?[67]	●		●	●	●			●		●	●	
Is technology that is designed to address violations of children's rights in digital environments, including digital learning, open source or shared, standardized, platform-agnostic, and available for use by all relevant and trustworthy parties involved, in all relevant sectors?[68]	●		●	●	●			●		●	●	
Are schools encouraged to seek and set up digital security mechanisms to ensure that only authorized individuals can access digital learning platforms and virtual learning environments?[69] What resources and support are provided for schools to do so and how is this monitored?	●		●		●			●	●		●	
How can schools ensure that platforms do not record sessions and store these recordings by default?[70]			●		●			●	●		●	
Do learning platforms, digital content, and any digital tool or service supporting education delivery signpost to reporting mechanisms[71]? Do they include clear instructions on whom to contact if parents, teachers or children have child-protection related concerns or complaints?		●	●	●				●	●		●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
What measures are in place by schools to ensure that children are kept safe when other means are used to reach out to children and their families, such as social media?[72] For example, what measures are in place to ensure safe livestreaming of classes via social media pages or to ensure that children are not recorded in any material that will be distributed, such as recordings of class sessions to be shared with students who were absent? If recordings are made that do include children, what measures are in place to ensure that written consent is obtained from parents/ caregivers and children's assent is obtained, that all parties know they can withdraw consent/ assent at any time, and that recordings that have been made but whose participants later withdrew consent/assent will be disposed of securely? Do schools have a policy that explains who is responsible for making, storing and disposing of recordings?			●	●				●	●			
Have all staff working on national and/or school-based learning management systems been trained in child protection? Is this training regularly updated as changes in digital learning development take place?	●		●					●	●	●	●	
Do the learning management system's administrator functionality, including user management, and user access controls take child online protection into account? Can administrators and users block and report content? Have national deployment and technical teams been working closely with child protection authorities to ensure Safety by Design of digital learning platforms and learning management systems?			●	●				●		●	●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are all child online protection features developed for digital learning platforms available on all versions of the platform (e.g., online, offline, web- and mobile-based) and in all languages in which the platform is available, i.e., in languages that children and their families speak and understand? Are the features accessible for children of all ages and abilities? If the platform or its contents have been developed in another context (e.g., another country), have child online protection features also been translated and contextualized for the local reality?			●					●		●	●	●
Are all child online protection features of digital learning platforms available also in instances when the platform is used to support digital learning for specific, vulnerable populations (e.g., for refugee children, in non-formal education contexts)?			●					●		●	●	●
Are human rights and Safety by Design standards at the centre of the design, development, deployment and functionality of learning management systems, digital learning platforms, digital resources and other tools to support digital learning?			●					●	●	●	●	
Are LMSs and digital platforms closely monitored for any content that is illegal, age-inappropriate, potentially dangerous or misleading, and for conduct that is illegal or harmful?			●					●	●	●	●	
Are any data collection processes and commercial practices related to learning management systems transparent, responsible, and in compliance with national and international laws and regulations?[73]	●		●					●			●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do digital learning platforms, tools, or resources use algorithms or other methods for filtering content[74]? If so, on what are these algorithms based? What processes are in place for ensuring that when aiming to personalize learning content, these filters do not isolate children or exclude them from accessing a wide variety of resources and ideas?	●		●					●			●	

4.2 Content and resources

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do national guidelines (e.g., recommendations, scorecards) for identifying, contextualizing and digitizing externally sourced learning content include considerations for age and developmental appropriateness, as well as safety and child online protection?			●	●				●		●		
Does digital learning content and content specifically designed to improve children's, teachers' and parents' awareness of online safety empower children to be aware, informed and able to act to identify and report risks or concerns?			●	●				●	●	●		●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are the criteria for the assessment of the safety of learning content made widely available and accessible, particularly to education service providers and content developers? Are child sexual abuse materials, the promotion or instruction of crime or violence on any scale, and the exploitative and offensive depictions of violence or sexual violence among the materials prohibited? Are the criteria for content a) developed by educational bodies, such as schools, b) intended primarily for children as an audience, and/or c) made available on or delivered by educational platforms the same as or stricter than the general criteria?	●		●			●		●	●	●	●	
Are resources, particularly educational materials for teachers, learners and parents/caregivers, and tools for addressing child protection risks online, particularly in digital learning, free and open-source? Are there tools or repositories for the sharing of such resources to avoid duplication of efforts and encourage collaboration among actors?	●		●	●						●	●	●
Are resources, particularly educational materials for teachers, learners and parents/caregivers, and tools for addressing child protection risks online, particularly in digital learning, co-developed, particularly with teachers, parents/caregivers and children and young people?	●		●	●						●	●	●
Do digital learning resources on child online protection for children, parents or teachers include diverse perspectives and represent diverse groups while being relevant to the local cultural, social and legal context in which they are being used? Have any resources provided from regional or global repositories or international content providers been translated, adapted and contextualized to ensure relevance to the lived reality of children, teachers or parents who are the intended audience?			●	●		●		●	●	●	●	●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are responsible digital engagement knowledge and behaviour, online safety, digital citizenship and critical digital literacy skills included and prioritized in digital skills development courses and materials? Do they cover the following areas: digital identity, digital use, digital safety, digital security, digital emotional intelligence, digital communication, digital literacy and digital rights[75]? Do these materials include relatable examples in a child-friendly, developmentally appropriate, and inclusive way? Do they include social and emotional learning that focuses on healthy relationships both online and offline? Have they been developed consultatively with experts on child online protection, learning and development?			●	●		●		●		●		
Does such content adequately represent the risks that children face, including from their point of view, and based on evidence? Does it include specific, action-oriented information on how children can contribute to safe online environments, how to identify unsafe content, behaviours or situations, how to protect themselves, and what to do if they feel unsafe or are exposed to unsafe content or situations?			●	●		●		●	●	●		●
Does such content address risks that are even more relevant for vulnerable groups, including children with disabilities, girls, children at-risk of dropping out of school, and children from the poorest families? Is it designed accordingly to principles of inclusion and Universal Design for Learning (UDL) and in the languages that children speak at home so that all children, especially those from more vulnerable groups, can meaningfully engage with and understand it?			●	●		●		●	●	●		●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Does this content explore issues, challenges, risks, and opportunities from a variety of angles, in a variety of contexts, and across a wide range of situations which children might encounter? Are both examples and non-examples provided and are key messages repeated and reinforced?[76]			●	●		●		●	●	●		
Are there standards against which such educational resources, whether developed locally, nationally or internationally, can be assessed to ensure accuracy and quality? Are teachers supported to co-develop these resources or their own and to access these standards for doing so?			●	●	●	●		●	●	●	●	
Is this content integrated with and across curricular subjects rather than being offered as stand-alone modules in ICT courses or through episodic events such as workshops or assemblies?			●			●		●	●			
Has a national curriculum mapping been conducted to identify how existing resources may be integrated across subjects and in support of national standards or learning outcomes?			●					●				
What pedagogical strategies are prioritized for the teaching of these skills and the use of such content in formal education? Do they rely on student engagement and child-centered learning rather than the transmission of information?			●			●		●	●	●		●
What professional development, support, resources, and guidance are available to ensure that these skills scaffolded and taught in a developmentally appropriate and progressive way rather than remaining static as children develop?			●			●		●	●			

4.3 Protection through digital learning

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are digital learning platforms being leveraged to deliver content and information on child online protection to teachers, parents and caregivers and children?	●		●	●		●	●	●	●	●	●	●
Are learning platforms being leveraged to promote and facilitate access to cost-free child safety referral services and helplines?[77]	●	●	●	●			●	●	●	●		
Is the information regularly updated to accommodate policy changes, the creation of new government functions, and to ensure all hyperlinks, such as to complaint mechanisms, are active and functioning?	●	●	●	●	●		●	●				
Access to reporting mechanisms, helplines, and information for directing children to legal services, law enforcement, and other support (e.g., counselling, safe houses) can be made available via digital learning platforms and other education-related services. Are such supports connected to regulatory services in order to streamline children's interactions with institutional bodies and services? Are they available in a confidential way for children who may not wish to discuss their need for these services and support with peers, parents, caregivers or teachers? Do they provide age appropriate support to children across the learning continuum?[78]	●	●	●	●	●		●	●	●	●		●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are any corporations whose platforms or tools are used for education delivery required to provide remedial and grievance mechanisms that are legitimate, accessible to all stakeholders (including teachers, learners, and parents), predictable, equitable, transparent, rights-compatible, and used for continuous learning (including for improving product safety)? Are these mechanisms safe, age- and developmentally-appropriate, responsive, and harmonized with rather than intended to circumvent reporting mechanisms established by relevant public sectors? Are users who access business-established grievance mechanisms still guaranteed access to courts, judicial review, and other procedures?[79]	●		●	●							●	
Are digital platforms leveraged effectively and efficiently to disseminate information on educational programs regarding child online safety?	●		●	●	●		●	●	●	●		●
Are learning management systems and digital platforms being leveraged to identify and mitigate child online protection risks? If so, how are children's data kept safe in these cases?	●		●	●	●			●	●	●	●	
How and to what extent is the potential of LMSs and digital platforms being leveraged to communicate about child online protection risks with learners, their families and the school community?	●		●	●	●			●	●	●	●	●

5. Teacher upskilling and support

This section takes a closer look at what measures may be put in place to ensure that teachers are prepared to identify and respond to child online protection concerns through teacher professional development and support and that accountabilities are clear.

5.1 Teacher professional development, support to teachers and accountability

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do pre-service teachers receive education and practical training explicitly related to keeping children safe online, including but not limited to the issues outlined in the previous question? Does this training specifically address the additional risks that children with disabilities, girls, refugee children and other vulnerable groups may experience, as well as how teachers can provide the additional support needed?			●			●		●	●	●		●
How are such competencies measured and is the demonstration of such competencies required for teacher certification?	●		●			●		●	●	●		●
Do in-service teachers receive regular (e.g., annual) training (or refresher courses) on the issues outlined above? How is this training funded? How is it quality-controlled? How is it certified?	●		●			●		●	●	●		●
How are such competencies measured and is the demonstration of such competencies required for teacher certification?	●		●			●		●	●	●		●
Is the percentage of teachers trained on child online protection monitored? What strategies are in place for increasing the percentage of the teaching cadre that has received certified, up-to-date training on the issues outlined above?	●		●			●		●	●	●		●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
By whom are these courses and training materials developed? Do the teams working on the development of these courses and materials include national and/or international experts related to both education and child protection? Have they been developed collaboratively with criminal justice experts or authorities and been approved by relevant ministries, such as Education, Social Affairs, and or Justice?		●	●	●		●		●	●	●		
Does the delivery of these courses include these experts as well, along with community-level actors such as law enforcement officers, and the voices of parents, teachers and children?		●	●	●		●		●	●	●		●
Are these courses and materials updated frequently enough to maintain relevance given the pace of change of the digital learning ecosystem, as well as any changes made to legislation and/or policy? Are teacher competency frameworks, pre- and in-service training requirements, and certification updated accordingly? Are there ongoing opportunities for support available to teachers, including mentoring, coaching, peer support and relevant and accessible websites with the latest news and guidance on child online protection?			●			●		●	●	●		
What support is available to educators to ensure that they can accurately deliver educational content, information and other relevant communication to parents, caregivers and learners about what child online protection involves, associated risks and mitigation measures, reporting procedures and processes, and the responsibility of different actors?[80]			●			●		●	●	●		●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
In addition to training on child online protection, do pre- and in-service teachers and other education actors receive mental health support to mitigate and respond to potential secondary trauma? Do policies exist that recognize and support teachers who have been exposed to secondary trauma, such as because of their students' exposure to sexual exploitation and abuse, including through digital learning? Have school leaders been trained to identify and respond to teachers' needs, such as through training and tools for recognizing and supporting teachers through stress, caretaker fatigue and secondary trauma?[81]	●		●	●		●	●	●	●	●		●
Are teachers and schools provided with reasonable means to access additional support for their learners, such as trained child protection specialists, and recovery and reintegration services and support, such as for children who may have been victims of violence, abuse or exploitation, including online and in digital learning?[82] Are such services made available to teachers, schools and learners, even when education is delivered at a distance?	●	●	●	●			●	●	●	●		●
What mechanisms are in place to assess and respond to teachers' and school leaders' needs related to child online protection training and support?	●		●			●		●	●			●
Conversely, are educators and education authorities involved in the creation of courses and materials for strengthening the capacity of relevant actors from other sectors to identify and mitigate child online protection risks and respond to child online protection concerns?		●	●	●			●	●				
For what elements of child online protection are teachers accountable? For what elements are schools accountable? To whom are they accountable and how are they held accountable? Are affected populations aware of this accountability and do they participate in it?	●	●	●	●			●	●	●			●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Do all teachers and education actors have a clear and accurate understanding of their responsibilities and the responsibilities of other actors in keeping children safe online? Whose responsibility is it to ensure that they do, and how is this enacted and monitored?	●	●	●	●			●	●	●			
What measures are in place to ensure that digital platforms that are used for facilitating home-to-school communication, teachers' communities of practice, mentoring, peer-to-peer support or other online interactions among teachers, education personnel, and families, where identifiable information about children might intentionally or unintentionally be shared even in children's absence, are safe and linked with reporting mechanisms? Are teachers aware of their responsibility to protect children's safety in such environments even when children are themselves not present?	●	●	●	●	●	●	●	●	●	●		●

6. Connectivity and devices

This section overviews key considerations for child online protection that must be taken into account in national and local efforts to increase access to devices and the Internet for learning. It covers efforts to bridge the digital divide as well as the safe use of the Internet and devices.

6.1 Bridging the digital divide

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Children and their families who have no internet or device access at home might not have had any prior exposure to information on online safety. Are efforts to increase device access, such as the distribution of devices to children and their families by the government or partners or the lending of devices to children by schools, paired with the distribution of educational materials on online safety in inclusive, accessible ways for children and their families?			●		●			●	●	●	●	
Are efforts to improve ICT infrastructure and schools' connectivity to the internet paired with a focus on child online protection, such as through training and capacity strengthening of all education staff and personnel, particularly in schools recently brought online?	●		●	●	●	●		●	●			
What measures are in place to ensure that internet access provided to children for educational purposes—such as through the provision of SIM cards or the zero-rating of educational content—does not inadvertently enable or support the unsafe use of the internet?	●		●	●	●			●	●			
Actors such as mobile network operators may be engaged in partnerships or efforts to expand internet access to children who do not have it to enable their participation in digital learning. What measures are in place to require these providers to offer families tools, services and configurations, such as safety features and parental controls?	●		●		●					●	●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
In cases where the government, partners, or educational actors including schools procure devices for distribution to learners, do minimum standards for these devices take both data security and child online protection risks into account?			●		●			●	●	●	●	

6.2 Safe use

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
How do schools and teachers support the safe use of devices during periods of distance learning?			●					●	●			
What procedures are in place to support families with keeping their children safe online when their children must use devices for learning unsupervised because of competing priorities (e.g., parents' work schedules)?	●		●	●	●			●	●	●		●
Has cooperation with telecommunications companies been pursued to encourage the waiving of costs for calls to child helplines, particularly by children, their families, teachers, and other education personnel, for example, via toll-free numbers?[83]			●		●			●			●	

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are teachers and school personnel authorized to use personal devices to communicate with children? If so, under which conditions and in which scenarios is this allowed? Is permission for the use of personal devices rather than organizational devices for this purpose granted on a case-by-base basis? Are records of this authorization, as well as clear protocol for who can view this communication, required and kept by the relevant staff? How are these communications monitored for language, conduct, content and risks?	●		●					●	●			

7. Support to parents, children and adolescents

This section presents questions for consideration in the development of digital learning strategies and plans. It presents reflections on the role that parents and children themselves play in keeping children safe online and aims to increase attention to empowering these key actors in the development of safe, inclusive digital learning ecosystems. It is divided into sections: Resources and learning; Monitoring and reporting incidents; and Advocacy and awareness raising.

7.1 Resources and learning

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
What support is provided to stakeholders and what training is provided to content developers to ensure the meaningful participation of teachers, parents and children in the development of resources on child online protection?			●	●	●						●	
Are resources available for parents of more vulnerable groups to support their safe online behaviour and minimize inadvertent risk exposure? For example, are parents of children with disabilities supported to identify safe online spaces in which they might seek support for their children and, on the other hand, to know when sharing information about their children and their disabilities might place these children at higher risk of adverse outcomes now or later?[84] How are such resources disseminated?			●	●	●		●	●	●	●	●	●
Are parent organizations, student councils, civil society organizations, and other local actors involved in outreach to ensure that the most marginalized families are included in efforts to strengthen parents' and children's knowledge on child online protection and that children who are the most vulnerable to these threats are reached?			●	●				●	●	●		●
How are digital learning platforms and tools being leveraged to provide or connect children with victim and survivor resources, including support groups, safe spaces, and professionally supervised peer-to-peer fora?[85]			●	●				●	●	●		●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
In what ways are education actors available and supported to encourage children and young people who have been exposed to child sexual abuse material to seek help, while at the same time, making them aware that they are engaging in illegal activity and may be held criminally responsible?	●	●	●					●	●	●		●
Do formal and non-formal opportunities for digital skills development, including those targeting the most marginalized children, include age appropriate elements of digital citizenship, online safety, responsible digital engagement and critical digital literacy skills? Do these cover the following areas: digital identify, digital use, digital safety, digital security, digital emotional intelligence, digital communication, digital literacy and digital rights?	●		●			●		●	●	●	●	●
Do youth engagement, volunteer programmes, and initiatives supporting youth-led entrepreneurship and innovation address digital skills, especially those for keeping children safe? How do mentorships, internships, apprenticeships, and other experiential learning opportunities to support young people, particularly those in which young people are engaged with the private sector, support the development of these skills?	●		●			●		●	●	●	●	●
Are children empowered to use their voices to support others at risk online or in need of help in a safe way?	●		●	●				●	●	●		●
What home-school communication processes and support are in place to share information about device settings, filters, child protection applications, and other tools and to support parents to effectively use these, particularly when devices are provided by the school and/or required for digital learning?[86] Do these include information on regular operating system updates and the use of security software?	●		●					●	●			●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are parents encouraged and supported by schools and teachers to communicate with their children openly about how and with whom children are communicating online, the type of interactions that are expected and appropriate, and what is inappropriate, harmful or discriminatory contact?[87]	●	●	●	●			●	●	●			●
Are codes of conduct for behaviour expected by students and teachers online clearly communicated, even when learning takes place at a distance? Are these expectations shared regularly, at least as often as schools transition to online learning, and (especially as digital learning may be used regularly to support in-person education delivery) are these codes of conduct consistently accessible?			●					●	●			●
Are guidance and rules for digital learning clear, consistent and not left open for interpretation? Are they formulated and delivered in a way that all children, especially children with disabilities or additional need for support, and their parents will be able to understand and apply?[88]			●					●	●			●

7.2 Monitoring and reporting incidents

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
In addition to national and industry reporting mechanisms, are there clear protocol in place at the level of the institution (e.g., school) that guide students, their families and teachers in reporting concerns about online risks in an offline way?								●	●	●		●
Is information that signposts to reporting mechanisms available in parent-friendly and child-friendly language, in the languages spoken by children and their families, and presented in multiple ways? Is this information available in both online and offline formats and responsive to the type of device used to access the learning platforms (i.e., is it available on both the mobile version and the desktop version of the learning platform)?			●					●		●	●	
Is any information related to child online protection delivered via digital learning platforms also delivered via other means, such as paper-based communication, to ensure accessibility by parents and caregivers who may not access the learning platform, particularly those from marginalized groups? Is this information available in multiple languages and multiple formats?			●					●	●	●		●
How are online communities of school members (e.g., teachers, parents, children) moderated and monitored? Is clear guidance published and easily and inclusively accessible?			●					●	●			●
To whom can parents, caregivers and children report concerns or incidents related to child online protection, especially if these are related to digital learning? What strategies are in place to ensure parents' and children's awareness and understanding of these issues and mechanisms?	●	●	●	●			●	●	●	●		●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are these reporting mechanisms inclusive and developmentally appropriate so that young children, children with disabilities—such as intellectual and developmental disabilities, visual impairments or other functional difficulties, and other particularly vulnerable groups can use them to report concerns or incidents? What efforts made to ensure that all children know how to and can do so?	●	●	●	●			●	●	●	●		●
Are these reporting mechanisms for child online protection concerns related to digital learning linked with other ways in which parents, caregivers and children engage in accountability regarding education and learning, such as feedback and complaint mechanisms?	●		●					●	●	●		●
Are there other mechanisms to enable all children and young people to safely voice their concerns and share information related to their experiences with using technology?	●		●	●	●		●	●	●	●		●
What tools and approaches are used for monitoring children's and parents' knowledge and engagement on these issues and their use of such mechanisms?	●		●	●	●	●	●	●	●	●	●	●
How can parents and children provide feedback on the relevance and effectiveness of such reporting mechanisms? Are they aware of this? Is their feedback regularly sought and incorporated into the design and implementation of these mechanisms?	●	●	●	●	●		●	●	●	●		●

7.3 Advocacy and awareness raising

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Have communication and advocacy campaigns been organized to widely share information about child online protection, targeting both parents/caregivers and children?			●	●	●		●	●		●	●	●
Do these campaigns address harmful social norms and behaviours, both online and offline, that contribute to child online protection risks, including as they relate to digital learning? Do these campaigns consider and accurately and effectively communicate the ways in which online behaviour can endanger children offline and vice versa? Do they avoid fear-based messaging and instead focus on empowerment and children's rights?			●	●	●		●	●		●	●	●
Do these campaigns use methods that can reach their target audience in multiple ways (i.e., not only online, via social media or on television)? Are they informed by data, such as through social listening, that provides information on parents/caregivers' and children's main concerns, as well as by data on the risks that children face?			●	●	●		●	●		●	●	●
What efforts have been made, working specifically with education stakeholders including children and parents as well as organizations and groups that represent their interests, to influence positive digital culture and safe digital behaviours?			●	●	●		●	●		●	●	●
What other social and behavioural change approaches have been used to spread awareness and empower children, parents and caregivers to prevent abuse and report suspected risks? What efforts have been undertaken to ensure children and parents are aware of their rights and the responsibility/accountability of the public and private sector to uphold children's rights and to safeguard them?			●	●	●		●	●		●	●	●

	Policymakers and legislators	Criminal justice	National education authorities	National child protection authorities	National ICT authorities	Teacher training institutes, research institutes, professional development providers	Municipal and local leadership	District and/or local education authorities (where relevant)	Schools	Other government partners (e.g., NGOs, CSOs)	Private sector (e.g., MNOs, private educational content providers, etc.)	Groups or representatives for parents, children and youth, and teachers
Question	**Audience**											
Are such approaches, campaigns and strategies developed and/or delivered in cooperation with education, child protection, and other relevant actors, including the private sector? Do they include, beyond schools, other channels to maximize reach, including industry, public institutions such as libraries and health centres, and other commonly frequented places?			●	●	●		●	●	●	●	●	●
Which education strategies and entry points are being leveraged for reducing the demand for harmful content, such as child sexual abuse material, and for raising children's awareness of their rights?	●		●	●	●		●	●	●	●	●	
Are children, including those from the most marginalized groups and most vulnerable to online risks, meaningfully engaged in the research and development of advocacy and policy around how the potential of ICTs can be harnessed while minimizing and responding to risks associated with digital technology?	●		●	●	●	●	●	●	●	●	●	●
Do schools communicate with parents/caregivers to make sure parents are fully aware of all individuals with whom children are expected to have contact for educational purposed, such as via digital learning platforms? Are online class schedules and schedules of any other online educational activities or expected communication, as well as contacts, shared with both parents and students?			●					●	●			●
What efforts are made to ensure that the aim of protecting children online, particularly in digital learning, does not suppress their natural curiosity, opportunities for innovation, socialization and access to peer networks, nor restrict other rights, such as freedom of expression, the right to access information, or the right to freedom of association? Are protection efforts and digital learning resources used to empower children to be resourceful and resilient in digital environments?[89]	●	●	●	●	●			●	●	●		●

Annex: List of additional resources

Research, Standards, Guidelines, Practices		
Title	**Source**	**Link**
Two Clicks Forward and One Click Back: Report on children with disabilities in the digital environment	Council of Europe	https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f
Releasing children's potential and minimizing risks ICTs, the Internet and violence against children	Office of the Special Representative of the Secretary-General on Violence Against Children	https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/6._releasing_childrens_potential_and_minimizing_risks_icts_fa_low_res.pdf
Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online	Broadband Commission for Sustainable Development, ITU, & UNESCO	https://unesdoc.unesco.org/ark:/48223/pf0000374365
UNICEF procedure for ethical standards in research, evaluation, data collection and analysis	UNICEF	https://www.unicef.org/media/54796/file
Guidelines for Industry on Child Online Protection	ITU	https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_E.PDF
Guidelines to respect, protect and fulfil the rights of the child in the digital environment	Council of Europe	https://www.coe.int/en/web/children/the-digital-environment
OECD Recommendation on Children in the Digital Environment	OECD	https://www.oecd.org/sti/ieconomy/protecting-children-online.htm
Protection from Sexual Exploitation and Abuse Technical Expert Group	Inter-Agency Standing Committee on Protection from Sexual Exploitation and Abuse (IASC-PSEA)	https://psea.interagencystandingcommittee.org/
Combating Online Child Sexual Abuse: Virtual Global Taskforce	Combating Online Child Sexual Abuse: Virtual Global Taskforce	http://virtualglobaltaskforce.com/
eSafety Commissioner	Australian Government	https://www.esafety.gov.au/
Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA: A Model National Response	WeProtect Global Alliance	https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf
Safety by Design (guidance)	Australian Government eSafety Commissioner	https://www.esafety.gov.au/sites/default/files/2019-10/LOG%207%20-Document8b.pdf

Codes, Legislation, International Conventions		
Title	**Source**	**Link**
Age-Appropriate Design: A Code of Practice for Online Services	UK Information Commissioner's Office	https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf
Harmful Digital Communications Act 2015	Parliamentary Counsel Office – Government of New Zealand	https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html
Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography	UN General Assembly	https://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx
Convention on Protection of Children against Sexual Exploitation and Sexual Abuse ("the Lanzarote Convention"	Council of Europe	https://www.coe.int/en/web/children/lanzarote-convention
Convention on Cybercrimes	Council of Europe	https://rm.coe.int/1680081561
Child Online Safety Universal Declaration	Broadband Commission for Sustainable Development, ITU, & UNESCO	https://www.broadbandcommission.org/wp-content/uploads/2021/02/WGChildOnlineSafety_Declaration2019-1.pdf
Writing Safeguarding Policies and Procedures	NSPCC	https://learning.nspcc.org.uk/safeguarding-child-protection/writing-a-safeguarding-policy-statement#article-top.com

Tools		
Title	**Source**	**Link**
Internet Literacy Handbook	Council of Europe	https://www.coe.int/en/web/children/internet-literacy-handbook
Digital Citizenship Education Handbook	Council of Europe	https://rm.coe.int/16809382f9.
Parenting in the Digital Age: Parental guidance for the online protection of children from sexual exploitation and sexual abuse	Council of Europe	https://rm.coe.int/parenting-in-the-digital-age-parental-guidance-for-the-online-protecti/16807670e8
Digital citizenship... and your child – What every parent needs to know and do	Council of Europe	https://edoc.coe.int/en/human-rights-democratic-citizenship-and-interculturalism/7865-digital-citizenship-and-your-child-what-every-parent-needs-to-know-and-do.html
Child Online Safety Index (COSI)	DQ Institute	https://live.dqinstitute.org/impact-measure/#:~:text=The%20Child%20Online%20Safety%20Index,part%20of%20the%20%23DQEveryChild%20initiative.

Tools		
Title	**Source**	**Link**
The International Child Sexual Exploitation image database	INTERPOL	https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database
Safeguarding and child protection self-assessment tool	NSPCC	https://learning.nspcc.org.uk/safeguarding-self-assessment-tool

References

[1] Hajela, S.K. (2018). *Policy considerations for AI governance.* Geneva: ITU. Available at https://www.itu.int/en/ITU-T/studygroups/2017-2020/03/Documents/Shailendra%20Hajela_Presentation.pdf

[2] United Nations Special Representative of the Secretary General on Violence Against Children. (n.d.). Bullying and cyberbullying. United Nations Special Representative of the Secretary-General on Violence against Children. https://violenceagainstchildren.un.org/content/bullying-and-cyberbullying-0

[3] UNICEF. (2018). Child safeguarding toolkit for business: A step-by-step guide to identifying and preventing risks to children who interact with your business. New York: UNICEF. Available at https://sites.unicef.org/csr/files/UNICEF_ChildSafeguardingToolkit_FINAL.PDF

[4] UNICEF. (2017). The state of the world's children 2017: Children in a digital world. New York: UNICEF. Available at https://www.unicef.org/media/48601/file

[5] UNICEF Division of Data, Research and Policy (DRP). (2015). UNICEF procedure for ethical standards in research, evaluation, data collection and analysis. Available at https://www.unicef.org/media/54796/file

[6] UNICEF. (2017). The state of the world's children 2017: Children in a digital world. New York: UNICEF. Available at https://www.unicef.org/media/48601/file.

[7] Ibid.

[8] International Telecommunications Union. (2011). ITU national cybersecurity strategy guide. Geneva: ITU. Available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

[9] United Nations Special Representative of the Secretary General on Violence Against Children. (n.d.). Bullying and cyberbullying. United Nations Special Representative of the Secretary-General on Violence against Children. https://violenceagainstchildren.un.org/content/bullying-and-cyberbullying-0

[10] International Association of Privacy Professionals. (n.d.). Glossary of privacy terms. IAPP Resource Center. https://iapp.org/resources/glossary/

[11] Council of Europe. (n.d.). Digital citizenship and digital citizenship education. Council of Europe. https://www.coe.int/en/web/digital-citizenship-education/home

[12] Fuller, S. (2021). Teachers' professional development modules: Formative assessment for quality, inclusive digital and distance learning during and beyond the COVID-19 pandemic. Learning guide for teachers. Geneva: UNICEF. Available at https://www.unicef.org/eca/media/19381/file

[13] European Commission. (2006). Ministerial Declaration – ICT for an inclusive society. Available at https://ec.europa.eu/information_society/activities/ict_psp/documents/declaration_riga.pdf

[14] UNICEF. (n.d.). Let's chat about online grooming. UNICEF Cambodia. https://www.unicef.org/cambodia/lets-chat-about-online-grooming#:~:text=Online%20grooming%20is%20sexual%20abuse,about%20their%20needs%20and%20vulnerabilities.

[15] International Telecommunications Union Development Sector ICT Applications and Cybersecurity Division. (2009). Understanding cybercrime: A guide for developing countries. Geneva: ITU. Available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

[16] UNICEF. (2021). Formative learning assessment in contexts of remote educational services in Latin America and the Caribbean: Literature review, guidelines and tools. Panama: UNICEF. https://www.unicef.org/lac/media/20736/file/Formative_Learning_Assesment_LAC.pdf

[17] UNICEF Division of Data, Research and Policy (DRP). (2015). UNICEF procedure for ethical standards in research, evaluation, data collection and analysis. Available at https://www.unicef.org/media/54796/file

[18] Australian Government eSafety Commissioner. (n.d.). Safety by Design. Australian Government eSafety Commissioner. https://www.esafety.gov.au/industry/safety-by-design

[19] U.S. Department of Commerce National Institute of Standards and Technology. (n.d.). Glossary. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/spam

[20] Bacon, K. (2014). All along: How a little idea called Universal Design for Learning has grown to become a big idea – elastic enough to fit every kid. Harvard Ed. Magazine. Available at https://www.gse.harvard.edu/news/ed/14/01/all-along

[21] ScienceDaily. (n.d.). Reference Terms. ScienceDaily. https://www.sciencedaily.com/terms/web_crawler.htm

[22] Body of European Regulators for Electronic Communications. (n.d.). What is zero-rating? Body of European Regulators for Electronic Communications. https://berec.europa.eu/eng/netneutrality/zero_rating/

[23] UNICEF. (2020). COVID-19 and its implications for protecting children online. Available at https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf

[24] Australian Government eSafety Commissioner. (n.d.). Safety by design. Available at https://www.esafety.gov.au/sites/default/files/2019-10/LOG%207%20-Document8b.pdf

[25] WeProtect Global Alliance. (2016). Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response. Available at https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf

[26] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Broadband Commission for Sustainable Development. (2019). Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online. Available at https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf

[31] Ibid.

[32] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[33] Livingstone, S. & Haddon, L. (2009). Introduction. In: Livingstone, Sonia and Haddon, Leslie, (eds.) Kids online: opportunities and risks for children. The Policy Press, Bristol, UK, pp. 1-6. Available at http://eprints.lse.ac.uk/30130/1/Kids_online_introduction_(LSERO).pdf

[34] UKCCIS Education Working Group. (2015). Online Safety in Education Report. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/517217/Online_Safety_in_Education_December_2015__2_.pdf

[35] Department of Infrastructure, Transport, Regional Development and Communications (n.d.). Current legislation. Australian Government. https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation

[36] The NSPCC. (2021, April 15). Social media and online safety. NSPCC Learning. https://learning.nspcc.org.uk/safeguarding-child-protection/social-media-and-online-safety#article-top

[37] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[38] Ibid.

[39] Livingstone, S. & Haddon, L. (2009). Introduction. In: Livingstone, Sonia and Haddon, Leslie, (eds.) Kids online: opportunities and risks for children. The Policy Press, Bristol, UK, pp. 1-6. Available at http://eprints.lse.ac.uk/30130/1/Kids_online_introduction_(LSERO).pdf

[40] International Telecommunications Union. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] WeProtect Global Alliance. (2021). Implementing the Global Strategic Response to Eliminate Child Sexual Exploitation and Abuse Online. Available at https://www.weprotect.org/library/guidance-for-implementing-the-global-strategic-response/

[45] Broadband Commission for Sustainable Development. (2019). Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online. Available at https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf

[46] WeProtect Global Alliance. (2016). Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response. Available at https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf

[47] WeProtect Global Alliance. (2021). Implementing the Global Strategic Response to Eliminate Child Sexual Exploitation and Abuse Online. Available at https://www.weprotect.org/library/guidance-for-implementing-the-global-strategic-response/

[48] European Commission. (2006). Ministerial Declaration – ICT for an inclusive society. Available at https://ec.europa.eu/information_society/activities/ict_psp/documents/declaration_riga.pdf

[49] Livingstone, S. & Haddon, L. (2009). Introduction. In: Livingstone, Sonia and Haddon, Leslie, (eds.) Kids online: opportunities and risks for children. The Policy Press, Bristol, UK, pp. 1-6. Available at http://eprints.lse.ac.uk/30130/1/Kids_online_introduction_(LSERO).pdf

[50] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[51] Ibid.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Office of the Special Representative of the Secretary-General on Violence Against Children. (2014). Releasing children's potential and minimizing risks ICTs, the Internet and violence against children. Available at https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/6._releasing_childrens_potential_and_minimizing_risks_icts_fa_low_res.pdf, (quote from p. 49)

[56] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[57] Livingstone, S. & Haddon, L. (2009). Introduction. In: Livingstone, Sonia and Haddon, Leslie, (eds.) Kids online: opportunities and risks for children. The Policy Press, Bristol, UK, pp. 1-6. Available at http://eprints.lse.ac.uk/30130/1/Kids_online_introduction_(LSERO).pdf

[58] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[59] Livingstone, S. & Haddon, L. (2009). Introduction. In: Livingstone, Sonia and Haddon, Leslie, (eds.) Kids online: opportunities and risks for children. The Policy Press, Bristol, UK, pp. 1-6. Available at http://eprints.lse.ac.uk/30130/1/Kids_online_introduction_(LSERO).pdf

[60] WeProtect Global Alliance. (2021). Implementing the Global Strategic Response to Eliminate Child Sexual Exploitation and Abuse Online. Available at https://www.weprotect.org/library/guidance-for-implementing-the-global-strategic-response/

[61] Ibid.

[62] Ibid.

[63] Ibid.

[64] Australian Government eSafety Commissioner. (n.d.). Safety by Design. Australian Government eSafety Commissioner. https://www.esafety.gov.au/industry/safety-by-design

[65] Broadband Commission for Sustainable Development. (2019). Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online. Available at https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf

[66] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[67] Broadband Commission for Sustainable Development. (2019). Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online. Available at https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf

[68] Ibid.

[69] Global Partnership to End Violence Against Children, ITU, UNESCO, UNICEF, UNODC, WeProtect Global Alliance, WHO, World Childhood Foundation. (2020). COVID-19 and its implications for protecting children online. Available at https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf

[70] Ibid.

[71] WeProtect Global Alliance. (2021). Implementing the Global Strategic Response to Eliminate Child Sexual Exploitation and Abuse Online. Available at https://www.weprotect.org/library/guidance-for-implementing-the-global-strategic-response/

[72] The NSPCC. (2021, April 15). Social media and online safety. NSPCC Learning. https://learning.nspcc.org.uk/safeguarding-child-protection/social-media-and-online-safety#article-top

[73] Global Partnership to End Violence Against Children, ITU, UNESCO, UNICEF, UNODC, WeProtect Global Alliance, WHO, World Childhood Foundation. (2020). COVID-19 and its implications for protecting children online. Available at https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf

[74] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[75] Ibid.

[76] Assiter, A., & Avery, R. (2018). Online safety for learners with special educational needs and disabilities. Education Safeguarding Service, the Education People. Available at https://www.kelsi.org.uk/__data/assets/pdf_file/0011/74576/Online-Safety-for-SEND.pdf

[77] Global Partnership to End Violence Against Children. (2020, July 21). Resources to make online platforms safe and accessible for children. End Violence Against Children. https://www.end-violence.org/articles/resources-make-online-platforms-safe-and-accessible-children

[78] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[79] Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, A/HRC/17/31 (2011), para. 31 https://digitallibrary.un.org/record/705860?ln=en#record-files-collapse-header

[80] WeProtect Global Alliance. (2021). Implementing the Global Strategic Response to Eliminate Child Sexual Exploitation and Abuse Online. Available at https://www.weprotect.org/library/guidance-for-implementing-the-global-strategic-response/

[81] Ibid.

[82] Office of the Special Representative of the Secretary-General on Violence Against Children. (2014). Releasing children's potential and minimizing risks: ICTs, the Internet and violence against children. New York: United Nations. Available at https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/6._releasing_childrens_potential_and_minimizing_risks_icts_fa_low_res.pdf

[83] Ibid.

[84] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[85] WeProtect Global Alliance. (2021). Implementing the Global Strategic Response to Eliminate Child Sexual Exploitation and Abuse Online. Available at https://www.weprotect.org/library/guidance-for-implementing-the-global-strategic-response/

[86] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

[87] Global Partnership to End Violence Against Children, ITU, UNESCO, UNICEF, UNODC, WeProtect Global Alliance, WHO, World Childhood Foundation. (2020). COVID-19 and its implications for protecting children online. Available at https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf

[88] Assiter, A., & Avery, R. (2018). Online safety for learners with special educational needs and disabilities. Education Safeguarding Service, the Education People. Available at https://www.kelsi.org.uk/__data/assets/pdf_file/0011/74576/Online-Safety-for-SEND.pdf

[89] ITU. (2020). Guidelines for policy-makers on child online protection. Geneva: ITU. Available at https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

unicef | for every child

United Nations Children’s Fund
Regional Office for Europe and Central Asia

Palais des Nations, CH-1211 Geneva 10, Switzerland
Phone: +41 22 909 5111
Email: ecaro@unicef.org
Website: www.unicef.org/eca/

**Funded by
the European Union**