unicef
for every child

Child Protection in Digital Education

Technical Note

CONTENTS

INTRODUCTION

> “States parties should develop evidence-based policies, standards and guidelines for schools and other relevant bodies responsible for procuring and using educational technologies and materials to enhance the provision of valuable educational benefits. **Standards for digital educational technologies should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to violence, discrimination, misuse of their personal data, commercial exploitation or other infringements of their rights**, such as the use of digital technologies to document a child’s activity and share it with parents or caregivers without the child’s knowledge or consent”. – Committee on the Rights of the Child, General comment No. 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para. 103 [emphasis added]

This technical note is intended to assist governments in ensuring that digital learning tools – also referred to as education technologies or ‘EdTech’ – introduced in schools promote equal and accessible education for all children and ensure the protection of children from the risks that the technology may introduce or amplify. While the primary audience is ministries and departments of education and ministries of children or equivalent, this note may also be useful for other public and private providers of educational and extra-curricula services and activities for children. For the most effective understanding of the issues, the technical note should be read together with the companion policy brief,[1] which offers concrete recommendations for education systems – i.e., teachers, school principals and leaders, school governing bodies, and government ministries (local, district and national) from early childhood education to the end of secondary school.

After briefly describing the risks that children may encounter with the use of digital technology in the education context, this technical note sets out eight key questions that policymakers should consider and offers guidance on how these questions can be navigated to keep children safe. A list of useful resources and a glossary of common terms are included at the end of the note.

[1] United Nations Children’s Fund, ‘Child Protection in Digital Education: Policy Brief’, UNICEF, New York, January 2023.

Understanding the risks that learners may encounter

Digital learning brings opportunities but also introduces risks that need to be managed effectively. The Committee on the Rights of the Child explicitly recognizes this in General comment No. 25:

> States parties should ensure the operation of effective child protection mechanisms online and safeguarding policies, while also respecting children's other rights, in all settings where children access the digital environment, which includes the home, **educational settings**, cybercafés, youth centres, libraries and health and alternative care settings.[2]

The introduction of digital technologies into learning, as in children's lives overall, brings with it new risks and new pathways to familiar risks. Risks may be introduced simply because the EdTech products and their terms and conditions have not been designed with children's rights in mind. **Online risks can be broadly classified according to the '4Cs' – contact, content, conduct and contract:**

Content: The child engages with or is exposed to potentially harmful content, e.g., not appropriate for their age, pornographic, violent, discriminatory or hateful.

Contact: The child experiences or is targeted by contact in a potentially harmful interaction, often but not always with an adult. These risks can lead to sexual exploitation, grooming, harassment, stalking, blackmail and other harms to children.

Conduct: The child witnesses, participates in or is a victim of potentially harmful conduct, e.g., bullying, sexting, image-based abuse, trolling, threats and intimidation, or is exposed to potentially harmful user communities such as those that promote self-harm or eating disorders.

Contract: The child is party to and/or exploited by a potentially harmful contract such as one that includes hidden costs or loss of control over personal data, or promotes commercial interests, e.g., targeted advertising, excessive use, gambling. These and other factors can be linked to insecure digital services that leave the child at risk of identity theft, fraud and scams, as well as poorly designed services that enable contracts between other parties to perpetrate child trafficking or sexual abuse.[3]

In the context of EdTech, there has been increasing attention to the misuse of children's data. While schools generally take steps to safeguard learners offline, they may be less likely to consider safeguards relating to the use of EdTech and other technologies that routinely collect children's data. **However, as technology is introduced into schools, efforts to protect children can only be effective if it takes into account these new technologies, services and platforms.**[4]

The introduction of EdTech may lead to the misuse of children's personal data, commercial exploitation or other infringements of children's rights.[5] This can involve, for example, the use of digital technologies to document a child's

[2] Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, United Nations, 2 March 2021, para. 26 [emphasis added].

[3] *Adapted from*: Livingstone, Sonia, and Mariya Stoilova, 'The 4Cs: Classifying online risk to children', Children Online: Research and Evidence (CO:RE), Hamburg, Germany, 2021, p. 11.

[4] *See, for example:* Turner, Sarah, Kruakae Pothong and Sonia Livingstone, 'Education Data Reality: The challenges for schools in managing children's education data', Digital Futures Commission and 5Rights Foundation, June 2022.

[5] *Examples of how governments and corporations collected data on a mass scale through EdTech have been documented through analyses of country strategies to introduce digital learning, and through examinations of the data collection and processing policies and practices of corporations.* See: Kwet, Michael, 'Operation Phakisa Education: Why a Secret? Mass surveillance, inequality, and race in South Africa's emerging national e-education system', *First Monday*, vol. 22, no. 12, 4 December 2017; and Hooper, Louise, Sonia Livingstone and Kruakae Pothong, 'Problems with Data Governance in UK Schools: The cases of Google Classroom and ClassDojo', Digital Futures Commission and 5Rights Foundation, 2022.

activity and share it with others who do not have any need to see or use these data without the child's or parent's knowledge. Some EdTech platforms, including those often recommended by governments and sometimes required by schools, routinely collect unnecessary data and sell data to third parties without their knowledge or consent.[6]

Although the right to privacy is increasingly protected in laws and regulations in many countries, and is covered broadly in the GDPR[7] and in COPPA,[8] the EdTech legal documents governing how children's education data are processed may contradict data protection regulations and may not provide sufficient transparency. Complicated and multilayered terms and conditions can appear to be like a 'jigsaw puzzle' for the governments, schools, teachers, parents and children that are trying to understand them.[9]

> **"Privacy is vital to children's agency, dignity and safety and for the exercise of their rights**. … Digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine. Such practices may lead to arbitrary or unlawful interference with children's right to privacy; they may have adverse consequences on children, which can continue to affect them at later stages of their lives." – Committee on the Rights of the Child, General comment No. 25, paras. 67, 68 [emphasis added]

Children may also be at increased risk of experiencing technology-facilitated child sexual abuse and exploitation, cyberbullying or self-harm with the introduction of EdTech, resulting in part from the increased time spent online, and the opportunities that these platforms can introduce for perpetration of abuse when not appropriately managed. There is also frequent concern about the impact of digital technology on children's mental health.

As children spend more time online, and technology becomes ever more central to their lives and their futures, they will be exposed to more risks. Equally, though, evidence indicates that as children become more digitally literate, they are more likely to successfully navigate some risks online without experiencing harm.

The distinction between risk and harm is significant: Not all risks will translate into actual harm for children, and encountering some level of risks – appropriate to their age and development – are important for children to learn how to successfully navigate difficult situations online, and develop resilience in the face of online risks. However, this is contingent on children being supported by parents and caregivers, educators and other responsible adults in their lives. It also does not take away from the crucial responsibility of identifying and mitigating those risks that cause harm to children.[10]

[6] Human Rights Watch, How Dare They Peep into My Private Life? Children's rights violations by governments that endorsed online learning during the Covid-19 pandemic, HRW, 2022, pp. 1–4.

[7] *The General Data Protection Regulation (GDPR) harmonizes data privacy laws across Europe and became applicable on 25 May 2018:* Intersoft Consulting, 'General Data Protection Regulation', Intersoft Consulting Services AG, Hamburg, Germany.

[8] *The Children's Online Privacy Protection Rule (COPPA) was finalized on 17 January 2013 and imposes certain requirements on operators of websites or online services directed to children under age 13, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under age 13*: Federal Trade Commission, 'Children's Online Privacy Protection Rule', FTC, Washington, D.C.

[9] Hooper, Louise, Sonia Livingstone and Kruakae Pothong, 'Problems with Data Governance in UK Schools: The cases of Google Classroom and ClassDojo', Digital Futures Commission and 5Rights Foundation, 2022, pp. 35–47.

[10] UNICEF Office of Research-Innocenti, 'Growing Up in a Connected World: Summary report', United Nations Children's Fund, Florence, Italy, p. 28.

Assessing, managing and responding to child protection risks associated with digital learning

This section presents eight key questions for policymakers to consider as they assess, manage and respond to child protection risks associated with digital learning. The content below each question offers guidance on how to answer these questions in ways that will keep children safe.

1 What policies and procedures have we established to ***evaluate the safety*** of EdTech prior to adoption?

Before introducing technology tools that will be used by and for children into the education system, it is essential to evaluate whether or not they are safe. Government policies and procedures should be established to guide such evaluations and should consider various dimensions of safety, including privacy, data protection, fairness and equity. **Sample questions to be considered when evaluating the safety of EdTech before adoption include:**

- *What features in EdTech apps and platforms are we going to allow?* Elements to consider include, for example, prohibiting disappearing messages, the potential risks of unrestricted communication between teachers and students, and guidelines for limiting the hours of use.
- *Who has access to the data that we are collecting and storing through the platforms and apps that we use?* It is essential to identify whether any third parties will be allowed access to students' data, either directly through the data collected by the application or platform, or through links to services external to the main EdTech platform, e.g., video-sharing sites or maps.
- *Do the EdTech apps and platforms we use allow for contact and communication between teachers and students outside of the requirement for teaching?* If so, the evaluation will need to consider whether these digital technologies could be misused by teachers.
- *Are there in-app or platform mechanisms for learners to report violence, abuse or exploitation by teachers or others?* Clear and accessible reporting pathways are a vital element of safeguarding children online.
- *Do the EdTech apps or platforms that we choose disadvantage any specific groups of students, such as those with disabilities or those who may be less digitally literate than their classmates?* Ideally, it would be best to select technologies that avoid discrimination, but if alternative platforms or apps are not available it will be necessary to identify how to alleviate any disadvantages, e.g., by providing options for personalized learning.
- *Do these apps or platforms make use of 'automated empathy', applying artificial intelligence (AI) to monitor students' emotions while learning?* [11] AI is increasingly used to assess children's attention, uncertainties or interest while learning by analysing recordings of their facial expressions, keyboard pressure or bodily movements. This technology is often packaged as enhancing the effectiveness of the learning platform as it offers teachers a way to gauge learners' response and progress. However, AI can discriminate against some users, often collecting unnecessary data on children and leading to 'false positives' in predicting certain behaviours or outcomes.[12] There are also

[11] Chan, Milly, 'This AI Reads Children's Emotions as They Learn', CNN Business, 17 February 2021; and McStay, Andrew, 'Hello Automated Empathy', Technology and Society, IEEE, 10 March 2021.

[12] *See, for example*: UNICEF Office of Global Insight and Policy, 'Policy Guidance on AI for Children', Version 2.0, United Nations

broader methodological and ethical issues with such technologies.[13]

When assessing data protection and privacy it is vital to look at both what happens within the EdTech services that are used in schools and what happens to children's data when links are made to other platforms. *(On effective approaches to assessment, see box 1, below.)*

Box 1: Age-appropriate technology

Significant strides have been made recently in the development of age-appropriate design codes in some jurisdictions[14] and methodologies such as privacy by design and safety by design – which encourage platform designers to assume, by default, that children will be the end users of the product and services, and to design these with children's safety and rights in mind.

Together with tools such as *child rights impact assessments* these design codes can provide an effective approach to assessing the suitability and safety of technology platforms for children, including EdTech.

As described in a recent study, for example, two of the biggest EdTech platforms kept children's data secure within the platform itself (the privacy-respecting 'core'), but any links or click-throughs to outside content such as videos or maps (the commercial 'additional' parts of the service) left the door open for collecting unknown quantities and types of personal data.[15] While teachers often use such content for illustration or educational purposes, and children may access these platforms as part of their learning experience, the boundaries between the EdTech itself and other content are frequently unclear. This makes it possible for data to be misused to, among other things, target children with inappropriate products, messages or other content that may pose a risk to their safety and well-being.

Responsibility for data: Technology companies often shift the responsibility for privacy and data protection onto the individual by requiring them to opt out of default settings.[16] The terms and conditions of some EdTech platforms place responsibility on schools to manage data within the platform,[17] often thus effectively limiting the company itself from liability. This means that it is up to the school to assess the risk posed to children. Ministries of education, and in turn schools, sometimes shift some of this responsibility onto parents and caregivers or children with little or no consideration of the disparate levels of digital literacy that may exist among the various users of digital learning technologies.

Studies have found that children – both boys and girls – trust their schools to keep them safe, and children use technologies required

Children's Fund, New York, 2021; and UNICEF Innovation and Human Rights Center UC Berkeley School of Law, 'Executive Summary: Artificial intelligence and children's rights', United Nations Children's Fund, Stockholm, May 2019.

[13] *See further*: UNICEF Office of Global Insight and Policy, 'Policy Guidance on AI for Children', Version 2.0, United Nations Children's Fund, New York, 2021, p. 21.

[14] *For example*: California Age-Appropriate Design Code Act, Assembly Bill No. 2273, 15 September 2022; and Information Commissioner's Office, 'Age-Appropriate Design: A code of practice for online services', United Kingdom, 2 September 2020. *For definitions of privacy and safety 'by design' see the glossary at the end of this technical note.*

[15] Hooper, Louise, Sonia Livingstone and Kruakae Pothong, 'Problems with Data Governance in UK Schools: The cases of Google Classroom and ClassDojo', Digital Futures Commission and 5Rights Foundation, 2022, pp. 9–10.

[16] *As noted in an exploration of children's experiences of social media in East Asia*: "Caught amid global platforms with limited to no protections for vulnerable young users, and in national contexts where the rule of law is weak, **there is an expectation of individual responsibility for data privacy without any actual transparency or ability to control social media platforms' data privacy practices**. Most of the children participating in our focus groups … had internalised messaging from tech companies and governments that limit the liability of companies and expect the individual to protect their privacy, even though the platforms make information public by default and are opaque about their data use practices." [emphasis added] Bulger, Monica, and Patrick Burton, ' "They Know Everything": Understandings of data privacy among teens in East Asia', London School of Economics and Political Science, 29 April 2020. See also: Stoilova, Mariya, Sonia Livingstone and Rishita Nandagiri, 'Children's Expectations Regarding Fair Treatment of Their Personal Data: What policy makers should know', London School of Economics and Political Science, 18 September 2019.

[17] Hooper, L., Livingstone, S., and Pothong, K., Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo. Digital Futures Commission, 5Rights Foundation, 2022, p. 9.

by the school assuming that these are safe. But children have also reported that they do not always trust the software they are directed to use by schools, and so take various steps to protect their own privacy, including password protection and blocking mechanisms. Learners have additionally mentioned that support from teachers, family and peers is an important way to improve online safety.[18]

Non-discrimination: In addition to data protection, any technologies to be used as learning tools should be evaluated to ensure they support fairness and equity. Even with the best of intentions, algorithmic biases in some platforms may place certain children at increased risk of being erroneously accused of misconduct, or predict poor performance or behaviour among certain groups of children – which can lead to marginalization or punishment.[19] These groups of children are often already facing discrimination as reflected in the data used to train the models. For example, children from minority groups or children who differ substantially from their peers are not usually represented in data sets. As a result, such systems may potentially reinforce stereotypes for children and limit children's opportunities.[20] In the context of education, this may not allow for the full range of learning styles and stream children into learning categories or opportunities that are not appropriate to their needs and talents.

Inequities in access and in digital literacy may also result in greater risks to some children's privacy. This often occurs not only as a result of disparities in access, skills and literacy that to a degree require a wider governmental response, but also due to algorithmic biases inherent in EdTech systems.

Girls, for example, may have lower levels of digital literacy due to fundamental gender disparities and may be at risk of poor education outcomes resulting from this. Children with disabilities, including physical, mental, intellectual or sensory impairments, may also have lower levels of digital literacy or encounter specific barriers that disadvantage them when learning shifts to EdTech. **These issues reinforce the importance of considering fairness and equity as well as data protection and privacy in evaluating the most appropriate platform or technology to use.**[21]

Children who are less familiar with technology and who do not know how to protect their own privacy may be at increased risk of harm. Reports have repeatedly highlighted that girls are systemically disadvantaged when it comes to developing digital skills, and so are often more likely to be at greater risk and more likely to experience harms from those risks than boys.[22]

Parents, caregivers and teachers as well as learners with lower levels of digital literacy may feel social pressure to opt in to features such as sharing photos or videos, even though they do not feel comfortable doing so or know that their privacy may be compromised. The 'end users' of digital technology often assume the responsibility for their own data protection, privacy and safety – viewing it as a personal

[18] UNICEF East Asia and the Pacific Regional Office and Young and Resilient Research Centre, 'Evaluating Online Safety Initiatives: Building the evidence base on what works to keep children safe online', United Nations Children's Fund, Bangkok, 2022, p. 19.

[19] Barrett, Lindsey, 'Governance of Student Data', Issue Brief No. 6, UNICEF Office of Global Insight and Policy, New York, December 2020, pp. 2–3.

[20] UNICEF Office of Global Insight and Policy, 'Policy Guidance on AI for Children', Version 2.0, United Nations Children's Fund, New York, 2021, p. 23.

[21] Vosloo, Steven, Melanie Penagos and Linda Raftree, 'COVID-19 and Children's Digital Privacy: How do we use technology and data to combat the outbreak now, without creating a "new normal" where children's privacy is under constant threat?', UNICEF Office of Global Insight and Policy, 7 April 2020. See also: Barrett, Lindsey, 'Governance of Student Data', Issue Brief No. 6, UNICEF Office of Global Insight and Policy, New York, December 2020

[22] United Nations Children's Fund, 'Policy Brief: Gender-responsive remote digital learning', UNICEF, New York, 2022, pp. 2, 1. See also: West, Mark, Rebecca Kraut and Han Ei Chew, I'd Blush If I Could: Closing gender divides in digital skills through education, EQUALS Global Partnership, 2019.

Box 2: Responsible Business Conduct –Core Frameworks

Since 2011, an authoritative framework defining States' duties to protect human rights in the context of business activities and relationships and the corporate responsibility to respect human rights has been provided by the UN Guiding Principles on Business and Human Rights.

The Committee on the Rights of the Child further outlines the roles and responsibilities of States in relation to the impact of businesses in General Comment 16.

responsibility rather than an obligation of the companies designing and providing the software or applications.[23]

However, the responsibility for data protection, privacy and platform safety should not be on parents and teachers. Rather than 'self-management', legal standards and voluntary best practices should focus on corporate behaviours.[24] Equally, governments have an obligation to develop and implement appropriate legislation, policies and regulations to ensure that companies take such actions, and to monitor and hold the technology sector accountable for doing so.[25] Ideally, the development of new frameworks to achieve better norms for responsible business conduct *(see box 2 above)* should entail consultation by policymakers, educators and civil society with industry, driven by experts devoted to the public interest rather than by the private sector.[26]

2 What policies and procedures have we established to ***manage the use*** of EdTech and digital communication tools in our schools?

The technology used for digital learning presents one set of risks, but how the technology is used may also expose children to unnecessary and inappropriate risks. These include how teachers choose to use the technology, and the boundaries and practices that are in place to guide teachers in their interaction with learners.

Even the use of everyday digital communication tools by class or parent groups can be an avenue for potential harm to children if they are not used thoughtfully and clear boundaries are not established. For example, the use of digital platforms to publicly shame learners, or to call individual learners out for bad behaviour or performance, can lead to stigma, bullying and social isolation. In the most extreme instances, it can lead to self-harm by the child or even suicide.[27]

Teachers and school staff may pose a direct threat to children, and have been responsible for violence and sexual abuse against students.[28] EdTech platforms and digital communication, like other technology and social media, may enable or facilitate violence, abuse or exploitation. These risks can be amplified in the absence of clear boundaries on acceptable use by teachers. For example, communication from a teacher to a student that occurs after school hours or beyond learning-at-home guidelines could establish or

[23] UNICEF East Asia and the Pacific Regional Office and the Centre for Justice and Crime Prevention, 'Our Lives Online: Use of social media by children and adolescents in East Asia – Opportunities, risks and harms', United Nations Children's Fund, Bangkok, 2020, p. 37.

[24] Barrett, Lindsey, 'Governance of Student Data', Issue Brief No. 6, UNICEF Office of Global Insight and Policy, New York, December 2020, p. 6

[25] Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, United Nations, 2 March 2021, paras. 36–39

[26] Barrett, Lindsey, 'Governance of Student Data', Issue Brief No. 6, UNICEF Office of Global Insight and Policy, New York, December 2020, p. 7.

[27] UNICEF East Asia and the Pacific Regional Office and the Centre for Justice and Crime Prevention, 'Our Lives Online: Use of social media by children and adolescents in East Asia – Opportunities, risks and harms', United Nations Children's Fund, Bangkok, 2020, p. 44.

[28] Know Violence in Childhood, Global Report 2017: Ending violence in childhood, Know Violence in Childhood, New Delhi, India, 2017, p. 5.

escalate inappropriate or unhealthy relationships, and may lead to abusive relationships, including sexual abuse.

To protect students from violence, abuse, exploitation and other risks, and to ensure they can benefit from the opportunities that EdTech offers for enhanced learning, it is crucial to develop and implement clear policies to guide acceptable use for all school-supported technologies.

Setting appropriate expectations and boundaries: Some schools have adopted programmes that monitor children's online activities, extending beyond school-related apps and into their social media and even texting behaviours.[29] These are often implemented for the perceived protection of children, but fail to ensure the appropriate safeguards for children's privacy and safety. Any such initiatives must ensure that they do not jeopardize or undermine the rights of children to privacy, information and play, and all other rights.

Where these programmes are adopted, parents, caregivers and children should all be explicitly informed of the extent to which the school is monitoring a child and for what purpose. Parents, caregivers and children also have a right to transparency on how these data are used, for example, if the data will be used to identify bullying behaviours, suicidal intentions or potential school violence.

In the case of video platforms, the assumption is that the links shared by teachers are only shared with learners. Yet unexpected interactions can also occur that could place children at risk. For example, during COVID-related school closures when children were attending classes via video platforms, any other person in the household could potentially view the child's screen. This may expose children to risks from people within households who may be involved in abusive or exploitative behaviour towards the child, as well as undermine children's right to privacy online. While enabling private rooms or chats can foster group work and project-based learning, it could also create opportunities for bullying.

Measures to codify expectations and boundaries relating to all aspects of digital technology and devices used in the classroom and throughout schools are vital and can be contained within policies and codes of conduct for children, learners and the school body as a whole. Acceptable use policies should be a central part of these measures. Where possible, children should be meaningfully involved in the development of these policies and empowered to determine the boundaries in terms of their own digital learning and interaction.

3 What technology infrastructure and policies do we have in place, other than those relating to EdTech, that will ***promote children's safety online*** when accessing the internet at school?

In addition to very clear policies relating to EdTech platforms, data protection and privacy, schools have a responsibility to provide safe networks and to take age-appropriate measures to protect children from specific sexual and other content, contact and conduct risks online.[30]

This may entail the use of firewalls to protect children from exposure to age-inappropriate content, as well as software protecting the network from viruses, phishing, malware and other malicious programmes. It should also

[29] *For two of the many examples emerging since the onset of COVID-19*, see: Human Rights Watch, How Dare They Peep into My Private Life?: Children's rights violations by governments that endorsed online learning during the COVID-19 pandemic, HRW, 2022; and Anand, Priya, and Mark Bergen, 'Big Teacher Is Watching: How AI spyware took over schools', Bloomberg, 28 October 2021.

[30] *See*: Livingstone, Sonia, and Mariya Stoilova, 'The 4Cs: Classifying online risk to children', Children Online: Research and Evidence (CO:RE), Hamburg, Germany, 2021.

take into account the consideration that **such tools should not infringe on children's other rights**, including the right to information and participation. *(See box 3, below, on upholding children's rights when employing technologies.)*

Box 3: Children's rights and digital technologies

As underscored by the Committee on the Rights of the Child, school safety-oriented technologies such as content controls and school filtering systems should not be used to restrict children's access to information in the digital environment. **They should only be used to prevent harmful material from reaching children.**

If digital surveillance of children is applied, it should always respect the child's right to privacy. Similarly, technologies that monitor online activities for safety purposes must be carefully implemented – particularly to ensure that they do not prevent a child from accessing a helpline or searching for sensitive information.[31]

4 How do we ***provide training and support for teachers and staff*** to use technology responsibly and appropriately?

Teachers are primarily responsible for using EdTech platforms, providing the interface between the technology and learners, and supporting learners. Yet in many contexts teachers view their learners as being more digitally literate than they are, and like many parents and caregivers may even rely on learners or their own children to show them how technology works.

Research across varied contexts shows that teachers often have limited technical skills. They may also be unaware of many of the risks that children can face, or how girls and boys experience risks differently and face diverse risks online. Equally, teachers are often unaware of the steps they can take on devices and platforms to keep children safe, or the most effective behavioural measures that can be taught and supported.[32]

When teachers are aware of risks online, they tend to be more alert to those that may result in the most severe harm, such as online grooming, sexual exploitation or cyberbullying. However, it is essential that teachers are supported in recognizing the wider range of risks that exist online, and how these may escalate or compound harmful outcomes for children.

While recognizing the benefits and opportunities that EdTech can bring to learners, teachers openly acknowledge the need for support and training, and may be left feeling disempowered without it. Training and support on how to use EdTech platforms in practice, e.g., organizing lessons, managing online classes, and simply using the technology are crucial,[33] along with specific training on how to ensure learners' safety.

The success and quality of EdTech take-up, implementation and the sustained safe use of digital learning in a way that effectively protects all the rights of the child – including the right to safety and protection – are largely dependent on continuous training, professional development and support for teachers.

[31] Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, United Nations, 2 March 2021, paras. 56, 75, 76.

[32] *See, for example:* Burton, Patrick, Miselo Bwalya and Sydney Sihubwa, 'Zambia Kids Online: A Global Kids Online study', Save the Children Zambia, Lusaka, April 2022; and UNICEF East Asia and the Pacific Regional Office and the Centre for Justice and Crime Prevention, 'Our Lives Online: Use of social media by children and adolescents in East Asia – Opportunities, risks and harms', United Nations Children's Fund, Bangkok, 2020.

[33] Pontuschka, Rafael, 'Listening to Children and Young People to Transform Education through Digital Learning in São Tomé and Príncipe', UNICEF Office of Research-Innocenti, Florence, Italy, 20 September 2022.

5 How are we ***communicating with parents and caregivers*** regarding the EdTech we are using in schools and supporting them in using this technology when learners are at home?

Parents and caregivers can sometimes lack the digital skills to provide support to their children and might not fully understand the risks that different technologies can present. Schools have an essential role to play in communicating clearly to inform parents and caregivers on:

- How the school is using EdTech and digital technology to benefit children's learning;
- The potential risks associated with using digital technology; and
- What the school is doing to ensure that children have equal access to the opportunities EdTech affords and that they stay safe online.

Part of this is equipping parents and caregivers with the skills and tools to support their children's use of EdTech in the home and make sure that their children's data are kept safe when using any school-supported digital technologies and platforms.[34] This is particularly important when parents and caregivers have limited technology skills. For example, they may feel undue pressure to provide consent to opt into video- or photo-sharing, and often do not know how to decline, opt out or ensure safety settings are on.[35]

Box 4: Adapting guidelines for safety

Several model guidelines for parents and caregivers on **keeping children safe online** have been developed in response to conditions during the COVID-19 pandemic.[36] While this guidance can provide a good entry point, schools – with support from districts and ministries – should develop and adapt it to include:

- Information on the choice and use of digital learning platforms;
- Expectations for parents, caregivers and students;
- What schools are doing to utilize these platforms safely; and
- How parents and caregivers can support the process, including localized resources for support.

While parents and caregivers generally know how to respond when their child experiences bullying or other forms of violence at school, they are less likely to know how to respond when their child experiences online violence, or when their data or privacy are compromised – or even that these incidents have occurred. Just as they would be informed of what measures are taken in response to misbehaviour, violence, poor discipline or any other threats relating to the child's well-being, safety and protection at school, parents and caregivers need detailed information on the policies and steps to take if their child experiences this online. *(For details on developing guidance in this regard, see box 4, above.)*

[34] *Examples of guidance for parents on keeping children safe online can be found in*: UNICEF East Asia and Pacific Regional Office, 'Tips for Parents and Caregivers: Keeping children safe online during the COVID-19 pandemic', United Nations Children's Fund, Bangkok, 2020.

[35] Krutka, Daniel G., Ryan M. Smits and Troy A. Willhelm, 'Don't Be Evil: Should we use Google in schools?', *TechTrends*, vol. 65, 2021, pp. 421–431.

[36] *For example:* UNICEF East Asia and Pacific Regional Office, 'Tips for Parents and Caregivers: Keeping children safe online during the COVID-19 pandemic', United Nations Children's Fund, Bangkok, 2020.

The onus is on the education system to help parents and caregivers in knowing how to identify instances of online abuse, exploitation or violence and how to respond. It is the responsibility of the relevant ministries to ensure that schools have adequate resources to provide this support.[37] Schools should also be responsible for setting and adhering to defaults within EdTech platforms and within the broader policies provided by ministries of education.

6 How are we ***communicating with children*** regarding the EdTech we are using and supporting them in using this technology?

Schools have a vital role to play in ensuring that children are equipped with the necessary skills to make informed decisions when online and to successfully navigate the risks they may encounter, while simultaneously making the most that being online has to offer – including the opportunity to participate in EdTech. Evidence shows that prevention education within schools offers one of the most effective approaches to keeping children safe online. This type of education should integrate content about online risks with offline violence prevention, given the overlap of these issues and their shared approaches to prevention.[38]

Children should be provided with support to become aware of the risks that the use of EdTech might introduce, understand how to manage those risks, and take proactive steps to stay safe when using digital learning platforms. **It is equally important that children learn when, how and where to report any misuse of EdTech or abuse that occurs through the platform.**

Research across regions shows that children are often hesitant to report any form of abuse that occurs online, including to schools. This reflects the global issue that violence remains 'hidden, unreported and under-recorded'. Many children are afraid to report incidents of violence against them because there is no safe or trusted way for children or adults to report it. They may also face stigma for reporting or be hindered by social acceptance of physical, sexual and psychological violence as 'normal'.[39]

A study on adolescents with mental health difficulties found that they face highly risky situations online and often have high levels of digital skills. But they did not feel that parents or teachers responded sensitively or effectively when they encounter abuse, leading them to keep their experiences secret. Safeguarding these and other vulnerable children online requires regulating and managing the digital environment to establish trust and meet their diverse needs,[40] including in EdTech and other digital learning platforms.

To overcome these barriers – including those that learners may experience using EdTech or digital communication platforms operated by schools – it is crucial for schools to:

- Encourage children to report online (as well as offline) abuse or violence;
- Provide safe spaces for them to report; and
- Ensure that appropriate action is taken in response to reports and is accompanied by adequate support services.

Box 5 *(on the following page)* describes the importance of listening to children about their own experiences.

[37] Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, United Nations, 2 March 2021, para. 102.

[38] *See*: World Health Organization, 'What Works to Prevent Online Violence against Children?: Executive summary', WHO, Geneva, 24 November 2022.

[39] Pinheiro, Paulo Sérgio, Report of the independent expert for the United Nations study on violence against children, A/61/299, United Nations, 29 August 2006, paras. 25–27.

[40] Livingstone, Sonia, et al., 'Young People Experiencing Internet-Related Mental Health Difficulties: The benefits and risks of digital skills', ySKILLS, KU Leuven, Leuven, Belgium, 9 August 2022, pp. 3, 5.

Box 5: Incorporating the voices of children

Children can provide unique insights into their experiences with digital technology, including EdTech, that is often different than adults' perceptions of their experience.

The Convention on the Rights of the Child, article 12, and the Committee on the Rights of the Child's General comment on children's rights in the digital environment (paragraph 16) call explicitly for children to be consulted in all matters that affect them, and their voices given due consideration in accordance with their age and maturity.

Children should be provided the opportunity to participate and be heard in the development of policies, legislation and programmes relating to their safety online and their use of EdTech. Accordingly, policymakers should give due weight to children's experiences.

7 What ***systems*** are in place for ***responding to violence, abuse or exploitation*** if it occurs within the EdTech apps or platforms?

As noted above, while EdTech and digital learning offer important opportunities and benefits, the potential also exists for abuse to occur, intentionally or unintentionally. Children who experience online harassment by another child or humiliation by teachers, or are drawn into abusive relationships with teachers, other adults or older children, must have appropriate recourse to report – and see appropriate action taken in response.

While each incident of abuse will require specific responses to meet the child's unique circumstance and needs, common elements will include the provision of psychosocial support, and in some instances, referral to both the broader child protection and criminal justice systems. **The responsibility is on the school, with support and guidance from the ministries of education, to develop response systems and embed these within the broader school safety and child safeguarding systems.** These systems should in turn be embedded within district or community safety and protection systems through which children affected can access support and remedy.[41]

8 Is ***online safety embedded*** in our broader school safety and child protection policies and strategies?

Evidence increasingly shows that the drivers of 'online' and 'offline' violence intersect or have similar impacts, and that a common approach is required to prevent and respond to risks and violence wherever they occur.[42]

This means that online safety – and in particular the identification, referral and provision of psychosocial support to learners – should be embedded within broader school safety policies and strategies rather than in a stand-alone policy. These policies should specifically designate responsibility for identifying and reporting the various forms of abuse or violence

[41] Children may face particular difficulties in obtaining remedy when their rights have been abused in the digital environment by businesses. For the obligations of States in this regard, see Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, United Nations, 2 March 2021, paras. 48-49 and Committee on the Rights of the Child, General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16, United Nations, 17 April 2013, paras. 66-67.

[42] UNICEF Office of Research – Innocenti, 'The Relationship Between Online and In-person Child Sexual Exploitation and Abuse', Disrupting Harm, *Data Insight* 6, Global Partnership to End Violence Against Children, 2022.

that may occur through digital learning and the use of EdTech.

Evidence from across the globe consistently shows that children rarely report incidents of violence, abuse or exploitation, either online or offline, to authority figures.[43] So schools, with support from ministries of education, have the responsibility to ensure that systems are in place to encourage and facilitate reporting. **Therefore, school safety or school child protection policies must contain specific reporting mechanisms that are accessible and user-friendly for all types of issues, including in the digital environment. Such mechanisms sit at the heart of school safety.**

Anonymous reporting should be enabled in these mechanisms, as social and cultural norms in some contexts may present additional barriers, particularly for girls and vulnerable groups of learners. Schools should also regularly assess what specific barriers children face in reporting, including through consultation with children, to determine if any individuals or groups face institutional or social deterrents to reporting. This can be done through reviews of school safety systems and monitoring mechanisms.

Reporting can also be encouraged through peer-support mechanisms and the identified responsible school leaders who can serve as intermediaries as and when needed. Once reporting has occurred, the school safety strategy or equivalent should detail very clear action and referral pathways for each report, where necessary integrating reporting of abuse through the digital platform as well. These referral pathways should have a direct link to social and protection services, including law enforcement for reportable offences. *(See the graphic at the end of this section.*)

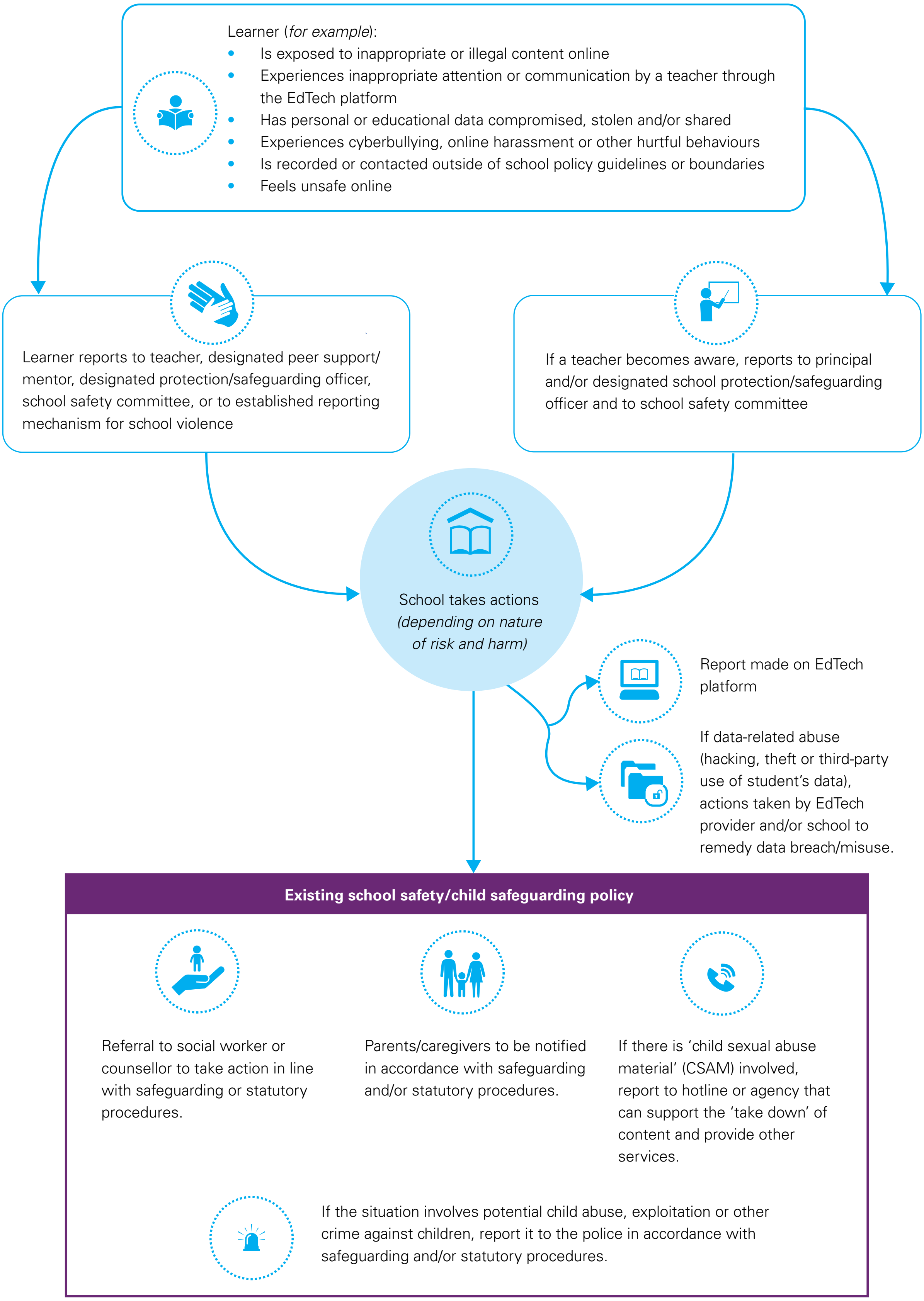
The response to abuse that occurs online, especially when it involves child sexual abuse materials or other forms of online child sexual exploitation and abuse, is often too narrowly focused and typically results in a take-down notice or other technological response from the platform or internet service provider. **Though frequently neglected, it is crucial to consider referrals to psychosocial support by schools and the EdTech platforms, and to the formal child protection system when necessary.** The overarching goals are to:

- Provide an appropriate and measured response to support the learner;
- Offer support to others who may have been affected by the incident; and
- Minimize the resulting harm.

The best way to achieve these goals is by making sure that school safety policies and strategies embed comprehensive, equitable and sensitive processes and pathways for reporting violence and abuse of any form that occurs through EdTech or any other digital platform used by the school.

[43] *For example*: UNICEF Office of Research-Innocenti, 'Children's Experiences of Online Sexual Exploitation and Abuse in 12 Countries in Eastern and Southern Africa and Southeast Asia', Disrupting Harm, *Data Insight 1*, Global Partnership to End Violence Against Children, 2022; and Ward, Catherine L., et al., 'Sexual Violence against Children in South Africa: A nationally representative cross-sectional study of prevalence and correlates', *The Lancet Global Health*, vol. 6, no. 4, 1 April 2018, pp. e460–e468.

Integrating identification and reporting of child protection concerns in relation to digital learning into school safety policies and processes:



Learner (*for example*):

- Is exposed to inappropriate or illegal content online
- Experiences inappropriate attention or communication by a teacher through the EdTech platform
- Has personal or educational data compromised, stolen and/or shared
- Experiences cyberbullying, online harassment or other hurtful behaviours
- Is recorded or contacted outside of school policy guidelines or boundaries
- Feels unsafe online

Learner reports to teacher, designated peer support/mentor, designated protection/safeguarding officer, school safety committee, or to established reporting mechanism for school violence

If a teacher becomes aware, reports to principal and/or designated school protection/safeguarding officer and to school safety committee

School takes actions *(depending on nature of risk and harm)*

Report made on EdTech platform

If data-related abuse (hacking, theft or third-party use of student's data), actions taken by EdTech provider and/or school to remedy data breach/misuse.

Existing school safety/child safeguarding policy

Referral to social worker or counsellor to take action in line with safeguarding or statutory procedures.

Parents/caregivers to be notified in accordance with safeguarding and/or statutory procedures.

If there is 'child sexual abuse material' (CSAM) involved, report to hotline or agency that can support the 'take down' of content and provide other services.

If the situation involves potential child abuse, exploitation or other crime against children, report it to the police in accordance with safeguarding and/or statutory procedures.

RESOURCES

- UNICEF, Gender-Responsive Digital Pedagogies: A guide for educators, June 2022
- UNICEF, Policy Brief: Gender-responsive remote digital learning, June 2022
- UNICEF Europe and Central Asia Regional Office, Child Online Protection in and through Digital Learning, May 2022
- UNICEF, Trends in digital personalized learning in low- and middle-income countries: Executive summary, May 2022
- Barrett, Lindsey, Governance of Student Data, December 2020
- UNICEF, The Case for Better Governance of Children's Data: A Manifesto, May 2021
- UNICEF and The GovLab, Responsible Data for Children website
- Digital Futures Commission and 5Rights Foundation, Education Data Futures: Critical, regulatory and practical reflections, 2022
- Digital Futures Commission and 5Rights Foundation, Education Data Reality: The challenge for schools in managing children's educational data, June 2022
- World Health Organization, What works to prevent violence against children online?, November 2022
- Safe to Learn, Supporting Schools to Provide a Safe Online Learning Experience, End Violence Against Children, May 2020
- UNICEF, COVID-19 and Its Implications for Protecting Children Online, April 2020
- UNICEF East Asia and Pacific Regional Office, Tips for Young People: Staying safe online during the COVID-19 pandemic, April 2020
- UNICEF East Asia and Pacific Regional Office, Tips for Parents and Caregivers: Keeping children safe online during the COVID-19 pandemic, 2020

GLOSSARY

Age-appropriate design refers to the consideration of the age of the end user of a product or service and the evolving capacities and developmental stages of a child, and associated risks, into the design and development of any new product or service. This ensures that the impact of a product or service on children of different ages is considered from the outset of the first development phase through to introduction and use of the product or service.

Algorithmic biases can be broadly described as inherent biases underpinning artificial intelligence, machine learning, digital technologies, apps or software that reflect entrenched social and structural inequalities and harmful norms. These usually result from the failure in the development and design of the products, in this case EdTech, to factor in inherent social biases within society in the datasets used to design the products or in how algorithms that process the data may be developed.

Child rights impact assessments in the business context can be defined as a process for identifying, understanding, assessing and addressing the adverse effects of a business project or business activities on children's rights.[44] Impact assessments can be considered as one tool within a wider child rights due diligence toolkit.[45]

Digital education: any teaching or learning process that entails the use of digital technologies, including online and offline formats, using distance, in-person or hybrid approaches.

Digital literacy refers to the knowledge, skills and attitudes that allow children to flourish and thrive in an increasingly global digital world, being both safe and empowered, in ways that are appropriate to their age and local cultures and contexts.[46]

Media literacy skills can be defined as the abilities to access, analyse, evaluate, create and act using all forms of communication. The purpose of media literacy education is to support learners' active inquiries and critical thinking about the messages they receive and create, with a focus on becoming informed and engaged participants in society.[47]

Education data: personal data collected from children at school and in school-supported online learning platforms whether in school or at home.

Personal data: information relating to an individual child which that allows them to be identified directly from that information or indirectly identified in combination with other information.[48]

[44] *Adapted from the definition of 'human rights impact assessment' in:* The Danish Institute for Human Rights, Guidance on human rights impact assessment of digital activities: Introduction, DIHR, 2020, p. 15. For more on the framework, scope and methodology for child rights impact assessments, see: Committee on the Rights of the Child, General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16, United Nations, 17 April 2013, paras. 50 and 62–65.

[45] *For further guidance on integrating children's rights within impact assessments, see:* UNICEF and The Danish Institute for Human Rights, Children's Rights in Impact Assessments, 2013.

[46] Nascimbeni, Fabio and Vosloo, Steven, 'Digital literacy for children: exploring definitions and frameworks, Scoping paper', UNICEF Office of Global Insight and Policy, New York, August 2019, p 31.

[47] National Association for Media Literacy Education, 'Snapshot 2019: The state of media literacy education in the U.S.', NAMLE, 2019, pp. 1, 2.

[48] *The definitions for 'personal data' and 'education data' were adapted from*: Day, Emma, 'Governance of Data for Children's Learning in UK State Schools', Digital Futures Commission and 5Rights Foundation, June 2021, pp. 10, 11.

Education system: In this technical note, the 'education system' includes teachers, school principals and leaders, school governing bodies, and government ministries at a local, district and national level – encompassing early childhood education through to the completion of secondary school.

EdTech: Education technology (EdTech) refers to the practice of using technology to support teaching and the effective day-to-day management of education institutions. It includes hardware (e.g., tablets, laptops or other digital devices), software, services and digital resources (e.g., platforms and content) that aid teaching, meet specific learning needs, and facilitate education institution operations. EdTech may also include the use of augmented, virtual and extended reality technologies as a means of enhancing learning.

Privacy by design refers to planning for and integrating privacy mechanisms into any app, software or product from the first stage of conceptualization and throughout design, development and production, thus ensuring that the privacy rights and needs of children are fully integrated into products from the start.

Safety by design refers to the same process of planning for and integrating safety mechanisms into any app, software or product starting with the first stage of conceptualization to ensure that the safety and protection rights and needs of children are fully integrated.

Referral pathways: the systems in place to report and refer any suspected or proven cases of violence or abuse of children to both the police and the child protection system. Most commonly, this will be the system that ensures that referrals are made from schools – and by teachers, principals, parents and caregivers – to school or other social workers, child protection officers or psychologists to ensure that victims receive the appropriate services, including psychosocial support.

School safety committees, also known as 'school child protection committees', are established at a school level and usually comprise representatives from: staff, such as a teacher and often the school counsellor if present; parents. frequently representing the school governing body; and students.

School safety framework, policy or strategy is a school-level tool that is used to diagnose and prioritize the safety concerns of learners, teachers and parents within a school. The framework, policy or strategy is used to develop a *school safety plan* to address these concerns, and to monitor progress of the implementation and outcomes of the school safety plan over time.

Technology-facilitated violence is the use of the internet and/or digital technology to bully, threaten, harass, groom, sexually abuse or sexually exploit a child.[49] It includes the production, possession, viewing and dissemination of child sexual abuse material (CSAM), which is the representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes, and any other form of child sexual exploitation and abuse that is partly or entirely facilitated by technology.[50]

[49] Radford, Lorraine, et al., Action to End Child Abuse and Exploitation: A review of the evidence, UNICEF Child Protection Section, Programme Division, New York, December 2020, p. 7.

[50] *Adapted from*: Committee on the Rights of the Child, Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/156, 10 September 2019, para. 60.

This technical note was researched and written by Patrick Burton with expert contributions and support from Dr. Monica Bulger. It was commissioned by the UNICEF Child Protection Team to support the work of UNICEF's Programme Group. Afrooz Kaviani Johnson, Child Protection Specialist, and Stephen Blight, Senior Child Protection Adviser, oversaw the technical note's development and provided guidance and support to the author.

Sincere appreciation is extended to all colleagues who provided advice and comments on draft versions, including:Samip Gupta, Antonia Mandry (UNICEF East Asia and the Pacific Regional Office), Jessica Katharine Brown (UNICEF Europe and Central Asia Regional Office), Katharina Wuppinger (UNICEF Middle East and North Africa Regional Office), Karin Heissler, Haritz Goya Lujambio, Catherine Muller, Kerry Neal (UNICEF West and Central Africa Regional Office), Line Baago-Rasmussen, Shiraz Chakera, Rachel Cooper, Frank Van Cappelle (UNICEF HQ)

Editor: Catherine Rutgers
Design: Mandy Lake

Suggested citation: United Nations Children's Fund, 'Child Protection in Digital Education: Technical Note', UNICEF, New York, January 2023.

Published by UNICEF Child Protection Team, 3 United Nations Plaza, New York, NY 10017.

Email: childprotection@unicef.org
Website: www.unicef.org

Cover photo: © UNICEF/UN0535990/Dejongh

A child attending class with her tablet at school in the South of Niger.

FOR EVERY CHILD, PROTECTION

unicef
for every child