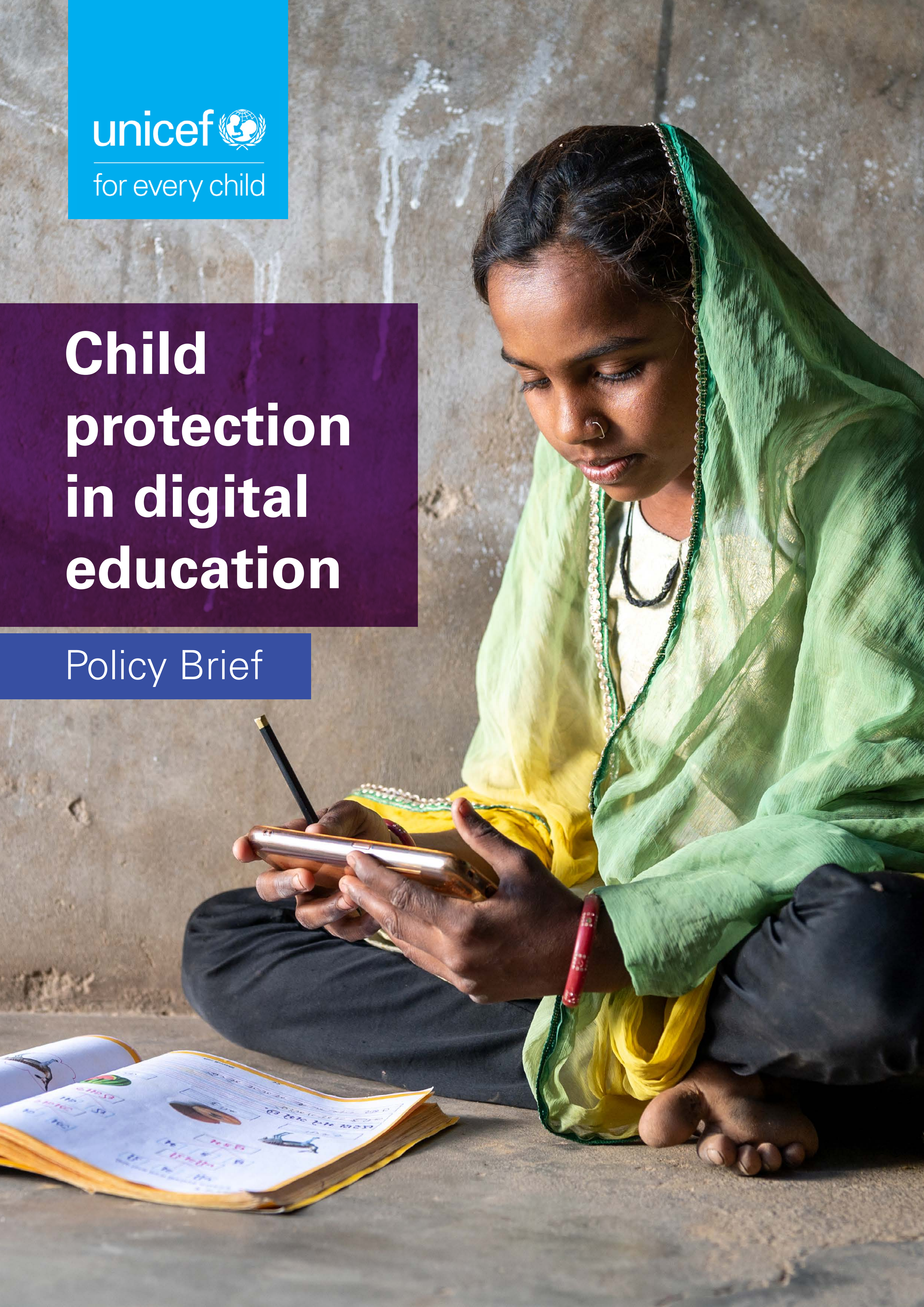
unicef

for every child

Child protection in digital education

Policy Brief



INTRODUCTION

The Convention on the Rights of the Child establishes the mandate to respect and ensure every child's right to education and to protection from all forms of violence. Over the past decade, schools have increasingly adopted the use of education technologies, or **EdTech**, to facilitate learning and teaching within schools. The impacts of the COVID-19 pandemic led to EdTech being introduced at an unprecedented rate in countries around the world. As teaching moved online during lockdowns, however, there was little guidance or support to ensure the safety and well-being of learners while delivering on their right to inclusive, equitable education.

This policy brief is intended to assist governments in ensuring that the introduction of EdTech and other digital learning tools by education systems promotes equal and accessible education for all children, and protects children from the risks that the use of technologies in schools may introduce or worsen. While television and radio are also used in many contexts for remote teaching and learning, the focus here is on digital technology.

The brief was developed to be particularly useful for ministries and departments of education and ministries of children or equivalent, and may also be applied by other public and private providers of educational and extra-curricula services and activities for children. For the most effective experience in using the policy brief, it should be read together with the associated technical note.[1] **Key terms are provided below, followed by five recommendations tailored to governments and/or schools.**

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

DEFINITION OF KEY TERMS

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.

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.

Education systems: In this policy brief, 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.

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

Personal data: information relating to an individual child that allows them to be directly identified from that information or indirectly identified in combination with other information.[2]

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.[3]

Media literacy skills can be defined as the ability to access, analyse, evaluate, create and act when using all forms of communication, including online and offline sources. 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.[4]

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.[5] 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

[2] *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.

[3] 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.

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

[5] 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.

partly or entirely facilitated by technology.[6]

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 – 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.

[6] 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.

RECOMMENDATIONS

for child protection in digital education

1 Governments should develop policies and procedures, with minimum standards, to ***evaluate the safety*** of EdTech prior to adoption and provide ongoing guidance for education systems on its use.

Ministries of education should have a *framework policy* that sets out what services and platforms are permissible, and what standards are required, in all EdTech to be used in education systems. Relevant mandates and expertise within the government should be engaged for policy development, including in relation to information and communication technology, cybersecurity, child protection and criminal justice. As part of the framework policy, all education authorities and schools under the ministry's purview should be required to develop policies and practices that conform with the framework.

Among other details to be underscored, EdTech data storage and sharing practices should not allow a third party to access sensitive information about students, including but not limited to disciplinary records, health information or their home address. 'Third parties' is defined as any person outside of those authorized within the school system to operate and/or utilize EdTech, and any company not directly providing the EdTech app.

The framework policy could also highlight applications or platforms with 'risky' design features. For example, applications or platforms that use or allow a vanish mode, in which messages disappear automatically, should be prohibited.

When assessing EdTech, government ministries will need to consider what happens to all data and information within the platforms used by schools. It is also necessary to consider what happens to children's data outside of the EdTech service itself when links are made to services or platforms where the protections safeguarding children's data are not followed, for example, when accessing video-sharing sites or maps. In addition, attention should be given to ensuring accessible reporting functions to report any abusive or inappropriate content or behaviour.

2 Governments and schools should develop policies, procedures and accountability mechanisms to ***manage the use*** of EdTech and all digital communication tools in schools.

These policies should include:

a) **Acceptable use –** An acceptable use policy should detail how teachers and school staff can use digital technology, including both EdTech and other digital communication tools and covering:

- How devices and the internet can be used;
- When during the school day they can be used;
- What devices and the internet can be used for; and

- Clear directions regarding what is not allowed.

Consequences for when the acceptable use is breached should be encompassed in the policy. Where possible, these consequences should avoid actions that would limit children's access and use of digital technology that would place them at a disadvantage to other children.

b) **EdTech use –** Boundaries for the use of EdTech should be set clearly, including:

- How and when teachers can contact learners;
- What data will be collected and by whom;
- Who will have access to that data; and
- How both education data and personal data will be used.

The policy should also define the obligations to report any misuse of the platform to school authorities, and where necessary, the wider child protection and criminal justice system. The expectations regarding how EdTech applications will be used should be provided, including what can be recorded, how these recordings are to be used and protected, and the limitations on recording.

The expectations for teachers, parents and caregivers and learners themselves should be clearly outlined, along with details on how the school will support parents, caregivers and learners in using the platforms at home.

All those who are affected by the use of EdTech in or through schools should be clearly notified regarding:

- How the technology is to be used;
- Why different features are used;
- What measures are in place to safeguard both children and their data; and
- What can be done when any misuse of the technology occurs.

c) **Reporting and help-seeking protocols –** Everyone who uses both EdTech and digital communication tools must be clearly informed about what they can do when they experience, witness or suspect that misuse of the technology is occurring.

To achieve this, schools should provide clear guidelines on how to report misuse, both within the app or platform itself and to the relevant school authority or designated child protection representative or officer. Reporting and help-seeking protocols should explicitly link to existing school safety policies, strategies or frameworks, and could be included in the 'EdTech use' policy described above.

These reporting protocols and systems should always be presented in a concise, easy-to-read format so that even those who may have limited understanding of digital technology are able to report using the appropriate channels.

Conveying essential information

Parents, caregivers and children should be explicitly notified regarding whether video or audio feeds from classes are recorded and if so, how the recordings are stored. It is equally important that parents/caregivers and learners know who will have access to the recordings, how long the recordings will be stored, and for what purpose. Ideally, nothing identifiable about the student is stored or shared.

They also need to be inclusive, for example, accessible to those children with disabilities, age-appropriate and in languages that are understood by parents and students. Where possible, reporting mechanisms should provide for some level of anonymity for the person making the report to minimize the possibility of stigma or re-victimization for reporting.

3 | Governments and schools should ***embed child online protection*** within broader school safety policies and strategies.

Each school must have a school safety policy, strategy or framework that establishes how the school is addressing learners' safety and creates the system for preventing, identifying, reporting and responding to all forms of violence. School safety policies, including those relating to technology-facilitated violence, should reflect the lived realities of all children, recognizing that different children may encounter risks differently and may be at greater risk of some forms of violence.

These policies should clearly identify:

- How and where different forms of violence should be reported;
- How each report will be dealt with; and
- The mechanisms for providing psychosocial support to learners when they experience violence.

Ideally, school safety policies should adopt a 'whole school' approach that seeks to promote a school climate and culture that is non-violent and inclusive. This entails being supportive and responsive to the needs of all within the school, taking into account the needs of the most marginalized, and addressing social and gender norms that foster violence, stereotypes and inequality.

Technology-facilitated violence is increasingly recognized as intersecting with other forms of violence and abuse experienced by children. This makes it crucial for the school safety system to cover all forms of exploitation and abuse that occur online or are facilitated by digital technology. For example, digital education policies should ensure that social norms fostering or enabling gender-based violence are challenged.[7] The school safety framework should also include details on how

Recognizing the signs of violence against children

There are common risks for violence that is committed with and without the use of digital technology that children might experience. This means that children who are at risk of experiencing violence, ranging from bullying to exploitation, are also likely to be at increased risk of violence committed using digital technology.

Many of the signs of abuse, exploitation or any form of violence experienced online are common to those of offline violence – isolation and withdrawal, poor or declining education performance, among others – and it is important that teachers know how to identify and respond to these potential indications of violence.

[7] See, for example: United Nations Children's Fund, 'Policy Brief: Gender-responsive remote digital learning', UNICEF, New York, 2022.

online risks and potential harms experienced by learners – both through the use of EdTech and more broadly – are to be reported and documented within the reporting system.

School safety strategies or policies should clearly identify institutionalized reporting mechanisms, both online and offline, and ensure that there are dedicated individuals who have participated in training on how to receive reports and how to make the necessary referrals for support. These individuals could be part of school safety or school child protection committees, or equivalent, where they exist. Peer mentors or counsellors can also receive training to provide referrals to the most appropriate adult. When peer mentors and support mechanisms are utilized, care must be taken to avoid placing undue pressure on the peer mentors/counsellors, and their role in providing referrals to trusted designated adults needs to be clearly delineated.

4 Governments and schools should provide ***training and support*** to school directors, teachers, parents, caregivers and learners on how to use EdTech, as well as other digital technologies, within the framework of the school policies on acceptable use, EdTech use and school safety.

Teachers often report that their learners know more about technology than they do, and in areas where internet and technology access may be new, teachers have very limited digital literacy skills of their own. **The responsibility is on schools, and on the ministries and departments of education under which they fall, to ensure that school administrations and teachers are adequately equipped to use EdTech and to support learners in their use of EdTech platforms.**

Different models can be used to build teachers' capacities, either by providing direct training and support, or by adopting an approach where teachers, parents and learners are taught collectively on the use of the technology and learn together. Whatever model is adopted, training should not be viewed as a one-time exercise – sustained training and support should be provided to teachers in the use of EdTech and digital learning. Training should also account for the fact that just as girls may be marginalized in access and use of technology, resulting in lower levels of digital skills and literacy,[8] female teachers may also be disadvantaged when compared to their male counterparts.

Training should cover a wide range of topics related to digital learning and online protection for learners as well as training on the EdTech platform being used, particularly in areas where teachers have limited digital skills. This could include, for example:

- Media literacy and digital literacy;
- The risks that children face online;
- How to identify children at risk of exploitation and abuse; and
- The referral and support mechanisms available both online and offline.

The specific measures that may be required to safeguard children when teaching remotely are also crucial elements to address, including

[8] United Nations Children's Fund, 'Policy Brief: Gender-responsive remote digital learning', UNICEF, New York, June 2022, p. 2.

the use of video, limits to recording of classes and students, and personal communication between teachers and students.

Teachers and parents must be clearly notified of what school policies and systems exist to guide the use of EdTech and other technologies within the school and when learning at home through the school. Schools should provide training for appropriate teacher-student and teacher-parent communication, including expectations and limiting teachers' communications to set hours to avoid establishing inappropriate or unhealthy relationships.

5 Schools should ensure that both platform and in-person ***reporting mechanisms*** are available and functional, and should actively promote and encourage their use.

Anyone concerned about the safety of a child should make a report to the designated school safeguarding or protection lead. Evaluation of the most appropriate EdTech technology to be used by schools should include the accessibility and functionality of reporting portals within the platforms and applications. Training on where these are located and how to use them should be provided to learners, parents, caregivers and teachers when the technology is introduced. Reports can also be made to reporting portals within the EdTech platforms.

All reporting mechanisms, online and in-person, should account for common barriers to reporting. These include barriers that may be faced by specific groups of learners, for example:

- Girls, who may not feel safe reporting to male teachers;
- Children with disabilities, who may not be able to navigate certain access points or platforms for reporting; and
- Cultural/linguistic minorities, internally displaced children and refugees, who may not feel safe reporting abuse or discrimination.

All reporting systems must ensure that designated reporting officials of all genders are available to facilitate reporting by children of violence they may otherwise feel uncomfortable or unsafe reporting.

Encouraging children to report incidents of violence or abuse

Evidence from around the world frequently shows that children rarely report technology-facilitated violence and abuse. Most commonly this is because they feel that nothing will be done about it, they fear being punished or re-victimized for reporting, or they do not consider it to be important. The same evidence exists for the lack of reporting of all forms of violence experienced by learners in schools. **Schools have a vital role to play in encouraging children to report and providing safe spaces for them to report – and in ensuring that appropriate action is taken in response to reports and support services are provided.** The same applies to abuse or violence that learners may experience using EdTech or digital communication platforms deployed by schools.

Keeping children safe while learning online, and using EdTech, should be integrated into school safety

Schools should think about the experiences that children have online – including through the use of EdTech and the process of digital learning – as just one aspect of their overall safety and well-being in school. Many of the harms that children experience in the digital environment are manifest in the same way as violence and abuse offline, and teachers can learn to identify these and other symptoms of abuse or trauma that children may exhibit.

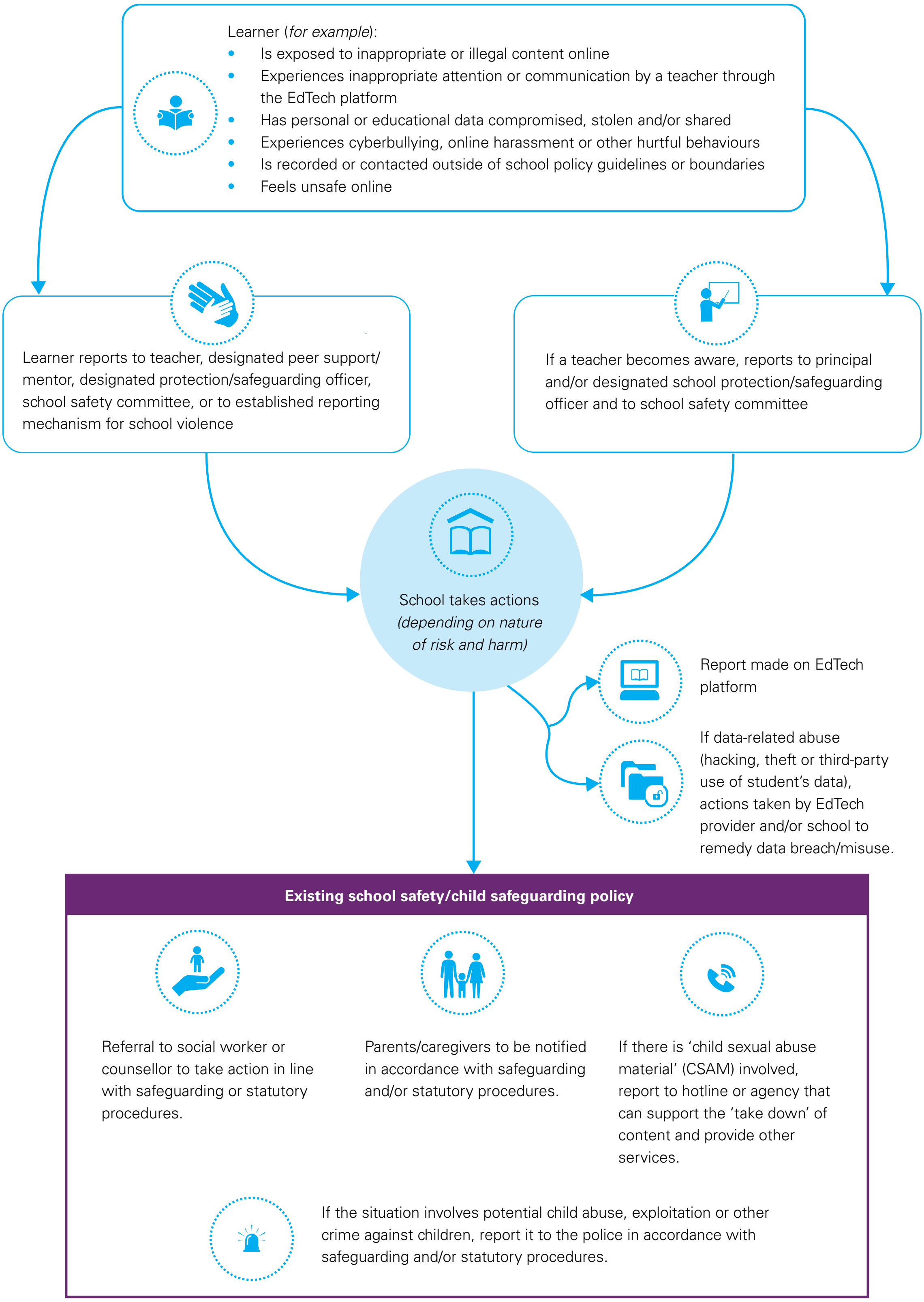
In response to the strong overlap between technology-facilitated violence and other types of violence, schools should integrate the identification and response systems for technology-facilitated violence into their systems for offline violence, such as school safety frameworks or strategies. This includes reporting and referral mechanisms, as illustrated in the graphic on the next page. It is crucial to equip teachers and bodies such as school safety committees with the tools they need to respond appropriately to all forms of technology-facilitated violence.

In practice, this may require updating the reporting and recording categories in school safety frameworks to include clear categories for violence or abuse perpetrated using digital technology, including EdTech. This information could also be incorporated into existing categories that are revised to enable an additional indication of where technology, and what technology, has been used.

Reporting systems should ideally be linked to referral mechanisms for psychosocial support and to the police when necessary. These mechanisms should enable reporting of abuse and misuse of personal or educational data, including data breaches. When data breaches have occurred, EdTech providers must be notified so they can take the required steps to correct and ensure that these violations do not happen again.

The integration of online protection and reporting, recording and referral mechanisms for technology-facilitated violence and abuse – including through the use of EdTech – into school safety strategies and policies *should always be done together with digital literacy and media literacy programming.* Integrating online safety and the teaching of skills that foster resilience, online and offline, into the formal curriculum and extra-curricular programming is an essential part of this process.

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.

This policy brief was researched and written by Patrick Burton with expert contributions 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 policy brief's development and provided technical guidance and support to the author.

Sincere appreciation is extended to all colleagues who shared valuable insights, 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: Policy Brief', 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/UN0378002/Panjwani
An 11-year old girl studies at home in Gujarat, India, as schools are closed due to the COVID-19 pandemic.

Page 2 photo: © UNICEF/UN0352054/Makyn
Students sit under a tree to use the internet while observing recommended social distancing at a school in Westmoreland Parish, Jamaica.

FOR EVERY CHILD, PROTECTION

unicef
for every child