



SAFE LEARNERS IN A DIGITAL WORLD

Adapting the Safe to Learn tools
to address technology-facilitated
violence in and around schools

Acknowledgments

This technical brief was developed by Catherine Flagothier, Safe to Learn Programme Specialist, and Afroz Kaviani Johnson, Child Protection Specialist, UNICEF, as lead co-authors.

The authors gratefully acknowledge the Safe to Learn partners for their valuable input and for shaping the concept of this Note, with particular thanks to members of the reference group: the CSO Forum to End Violence Against Children, the Global Partnership for Education, Safe Online, Together for Girls, UNESCO, UNGEI, and UNICEF. With thanks also to the UNICEF peer reviewers, and special appreciation to Gemma Wilson-Clark, Head of the Safe to Learn Secretariat, for her strategic guidance and review.

Design by Big Yellow Taxi, Inc.
June 2026

Cover photo: © UNICEF/UN0825676/Das

Table of Contents

Acknowledgments	2
Introduction	4
Purpose	4
Why integrate digital safety into Safe to Learn?	5
What risks do digital technologies introduce for learners?	5
Why is the role of education critical in preventing and responding to these risks?	6
How can digital safety be integrated into existing efforts to protect children in, around, and through schools?	7
Call to Action Area 1: Implement laws and policies	8
Call to Action Area 2: Strengthen prevention, risk mitigation and response in education systems and at the school level	8
Call to Action Area 3: Shift social and gender norms and promote behaviour change	9
Call to Action Area 4: Invest resources effectively	10
Call to Action Area 5: Generate and use evidence	10
Annex	11
Safe to Learn Benchmarks: integrating components on prevention and response to technology-facilitated violence	11
Key references	16
Additional references	16
Endnotes	17

Introduction

Safe to Learn is a global initiative that brings together governments, civil society, United Nations agencies, donors, global partnerships, and the private sector to end violence in, around, and through schools, so that all children can learn in safe and enabling environments. Violence in and around schools undermines learning outcomes, mental health, and children's rights, making coordinated action and inter-sectoral collaboration essential.

Through its technical package – including the Safe to Learn [Call to Action](#), [Programmatic Framework and Benchmarking Tool](#) and [Diagnostic Tool](#), Safe to Learn helps countries identify gaps, set priorities, monitor progress, and design and implement evidence-informed policies and programmes.¹ By fostering collaboration, the initiative aims to create learning environments where every child feels safe, respected, and empowered to thrive.

Purpose

The rapid expansion of digital technologies has transformed how children learn, communicate, and interact, increasing both their online presence and their exposure to risks. While the Safe to Learn technical package already references online safety, the fast pace of technological change, including artificial intelligence (AI), highlights the need to further adapt and strengthen Safe to Learn's tools to support governments in ensuring safe and enabling learning environments, including through digital technologies.

This Technical Brief is structured around the Safe to Learn Call to Action, showing how each Call to Action area and its benchmarks can be strengthened to better address digital risks in, around, and through schools. It draws on the Safe to Learn technical package and [UNICEF's global guidance on child protection in digital education](#) and is designed to support countries and partners across all contexts. Rather than serving as an operational manual, this brief provides a framework and illustrative guidance to help countries integrate digital safety into national laws and policies, school practices, whole-school interventions, budgets, data and multi-sectoral systems.²



Why integrate digital safety into Safe to Learn?³

Digital technologies are increasingly inseparable from how children learn, play, and socialize. They can enhance access to learning, foster creative and critical thinking, support learner participation and help build resilience and agency, particularly when embedded within safe, inclusive school systems. However, they can also enable, aggravate, and amplify violence against children, including bullying, gender-based violence, sexual exploitation and abuse, and exposure to harmful content. Governments should therefore

embed digital safety, proactively and by design, across the education system – from national policy to school-level practice. For instance, [UNICEF's Digital Education Strategy 2025-2030](#) highlights a lack of standards around safe and effective use of digital in education. By integrating digital safety into Safe to Learn's tools, governments and partners can strengthen existing interventions by considering digital dimensions to ensure children are protected in both online and in-person education settings.

What risks do digital technologies introduce for learners?

Learners face a range of risks through digital technologies both in and around schools. The commonly used '5Cs' provide a helpful categorization of online risks, encompassing:

- **Content** – harmful material children may see online such as violence and pornography
- **Contact** – harmful interactions such as grooming or exploitation
- **Conduct** – harmful peer behaviour such as cyberbullying
- **Contract/consumer** – commercial risks and misuse of personal data
- **Cross-cutting risks** – affecting children's privacy, mental health and well-being⁴

The rapid expansion of education technology ('EdTech') during and after COVID-19 heightened these risks and revealed governance gaps.⁵ More recently, schools worldwide have been grappling with emerging forms of technology-facilitated violence, including peer-to-peer violence enabled by generative AI – such as so-called 'nudify'/'undress' applications and deepfake tools.⁶



© UNICEF/UN0535990/DEJONGH

Why is the role of education critical in preventing and responding to these risks?

Safe and enabling learning environments are essential to breaking the cycle of violence. They are globally recognized as one of the three high-impact solutions to effectively prevent and respond to violence against children, alongside parenting support and response services.⁷ Learning environments are becoming increasingly intertwined with the digital environment, and persistent digital divides remain across countries and communities.⁸ Children spend more time online, whether through personal devices or digital tools provided by schools. Closing these digital divides is central to achieving equity in learning. Equally essential is ensuring that, as access expands, digital safety is embedded from the outset so that children can benefit from technology without exposure to technology-facilitated violence.

This places a responsibility on schools to ensure learners are safe not only on their physical premises but also in digital spaces connected to school life. As one of the most influential institutions in children's lives after the family, schools are uniquely positioned to empower children with the knowledge, skills, and support needed to navigate digital environments safely and responsibly.⁹ Teachers and school staff play a key role in both violence prevention and early responses, as they are often the first to observe signs of harm. Schools should be equipped to provide guidance, frontline support, and referrals to specialized services for children. This includes child protection services and mental health and psychosocial support (MHPSS). This role is reinforced by several UN authoritative normative documents, and high-level political commitments.¹⁰

Box 1: Note on terminology

This Technical Brief primarily uses the term **'technology-facilitated violence against children'** instead of **'online violence,'** as it more accurately encompasses all forms of violence, abuse, and exploitation that are perpetrated in part or fully through digital technologies, not just those occurring on the internet. It reflects the varied and evolving ways technology is being used to harm children.¹¹ It also guards against binary notions of **'online'** and **'offline'** harms. The increasing role of technology in children's lives means that drawing a clear line between **'online'** and **'offline'** forms of violence is neither conceptually possible nor of practical use.¹²



How can digital safety be integrated into existing efforts to protect children in, around, and through schools?

The following section sets out how to integrate digital risks into the Call to Action areas of Safe to Learn. It includes strategies already referenced in the Safe to Learn programmatic framework as well as new strategies to be included in its forthcoming revised edition.

The Safe to Learn Programmatic Framework translates the Call to Action into a set of 'Benchmarks' informed by international child rights frameworks, UN guidance and minimum standards, and good practices from the field of child safeguarding and child protection. The benchmarks highlight what needs to happen for each Call to Action area to be realized. Call to Action areas, as well as benchmarks, are closely connected. While guidance and strategies proposed in this brief have been allocated to particular benchmarks for the sake of clarity, many could appropriately be situated across multiple areas of the framework. See also Annex 1, which sets out how digital safety and prevention and response to technology-facilitated violence could be considered within the Safe to Learn benchmarks.

Box 2: A whole-school approach

As with tackling any form of violence, abuse and exploitation, it is essential to take a 'whole-school approach' to address risks that arise in relation to digital technologies. A whole-school approach integrates policies, teaching practices, student participation, reporting systems, and community engagement, ensuring that teachers, learners, parents and caregivers, and school leaders collectively share responsibility for preventing harm and promoting well-being. Rather than treating digital safety as a one-off lesson, this approach makes it a core part of school culture and daily practice, in line with the [Safe to Learn Call to Action](#) and [Global minimum standards from a whole school approach to prevent school-related gender-based violence](#).¹³





CALL TO ACTION AREA 1: **Implement laws and policies**

National policies and legislation to tackle violence in and around schools should explicitly address technology-facilitated violence. The Safe to Learn technical package already stresses the importance of considering both 'online' and 'offline' violence in education sector analyses, policy reviews, and planning processes. Building on this foundation, education sector policies and plans should integrate technology-facilitated violence within broader violence prevention strategies. These policies should be technology 'neutral,' meaning they are not focused on specific platforms, apps or tools but instead focus on the principles and outcomes, ensuring that protections apply across current, emerging and future technologies.

Ministries of education should also ensure technology-facilitated violence is included in national child protection/safeguarding policies, with due consideration of children facing multiple forms of discrimination. Existing multi-sectoral referral mechanisms need updating to ensure education authorities, schools, and

teachers have defined roles, mandates and obligations in responding to technology-facilitated harm - including harm perpetrated by students -and established points of contact with cybercrime units, helplines, hotlines, and platform escalation channels.

Ministries of Education should introduce a framework policy that defines which services and platforms are approved for procurement and use in educational settings, with minimum standards such as safety-by-design, privacy-by-default settings, age-appropriate design, and prohibitions on targeted advertising or manipulative design features. They should mandate robust child rights governance measures (e.g., due diligence and data protection impact assessments) before approving any digital learning tools and maintain an official list of approved platforms that meet these standards.¹⁴ UNICEF's [EdTech for Good Framework](#) enables the evaluation and curation of safe, impactful and scalable digital learning tools.¹⁵



CALL TO ACTION AREA 2: **Strengthen prevention, risk mitigation and response in education systems and at the school level**

Schools and education systems should adopt a whole-school approach to online safety (see Box 2). Existing Safe to Learn guidance calls for integrating violence prevention into student curricula, strengthening teacher training, and promoting safe behaviours. Building on this foundation, education systems should ensure that these measures address the realities of digital environments. This includes integrating digital literacy and safety into national primary and secondary curricula, ensuring materials are culturally appropriate and suitable for children's age and stage. Content should include respectful online behaviour, cyberbullying prevention, technology-facilitated gender-based violence, consent, image-sharing and scam awareness, alongside strategies to support help-seeking.¹⁶ The provision of age-appropriate and culturally relevant life skills training and centred on empowerment, critical thinking and the promotion of gender-equitable norms and power relations is also important to encourage open dialogue about healthy relationships.^{17,18} It can help children recognize the

warning signs of predatory or harmful behaviours, both in-person and through digital technologies.

Child safeguarding principles, policies, procedures and frameworks must integrate digital safety, including clear standards on acceptable use, device management, classroom streaming and recording, data handling, and screening for roles involving online access to children. Child-friendly reporting and support systems should be accessible both online and in-person, linked to national referral pathways. Codes of conduct and teacher professional standards must reflect digital dimensions, including clear rules on out-of-hours communication. Teachers, counsellors and staff require pre-service training and in-service professional development on technology-facilitated harms, child safeguarding, data protection, and education technologies, while parents and caregivers should receive regular updates and information on school use of technologies and safeguarding processes.



CALL TO ACTION AREA 3: **Shift social and gender norms and promote behaviour change**

Efforts to transform harmful social and gender norms must extend to digital spaces, where gender stereotypes, discrimination, and violence are often amplified. Whole-school approaches that engage teachers, school staff, school management, learners, parents, and caregivers should explicitly address technology-facilitated violence, including technology-facilitated gender-based violence. Building on the existing Safe to Learn guidance, parent-teacher associations and school management committees should be strengthened to understand and address online risks and support efforts to prevent and respond to all forms of violence, including those perpetrated through technology. Schools should foster active student leadership and support peer-to-peer initiatives that promote positive online behaviours.

Education authorities should commission and endorse evidence-based initiatives that address harmful social and gender norms driving violence, including technology-facilitated violence, and examine differentiated risk factors in digital environments. Schools should also engage learners, families, and communities in dialogue and joint action to challenge harmful social and gender norms that drive violence, both in-person and through technologies – ensuring that interventions are culturally relevant and inclusive. Anti-bullying and norm-change initiatives should expressly incorporate the digital environment. Data on the nature, incidence, impacts, and costs of school violence, including technology-facilitated violence, should be used to raise awareness among teachers, parents, policymakers, donors, media and wider communities, and to advocate for change.

“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.”¹⁹

UN Committee on the Rights of the Child, General comment No. 25 (2021) on children’s rights in relation to the digital environment





CALL TO ACTION AREA 4: **Invest resources effectively**

Sustained investment is essential to ensure that education systems can prevent and respond to technology-facilitated violence. Evidence, including data on the costs and impacts of online violence, should be generated and used to advocate for increased and improved public financing. Dedicated budget lines at the national, sub-national and school level to integrate digital safety are essential. These should cover necessary costs such as teacher training, content filtering, and vendor compliance audits.

Shared-value partnerships can also play an important role. Building on existing Safe to Learn guidance, UNICEF and partners can leverage private-sector expertise,

technology and operational capacity to strengthen efforts to address technology-facilitated violence. Partnerships with relevant companies can support safe connectivity and device management as well as broader efforts to address technology-facilitated violence in and around schools. Procurement processes should also embed safety and privacy criteria into contracts, with requirements for independent audits of EdTech and other relevant providers. Development partner resources should be leveraged to integrate digital safety into sustainable systems for preventing and responding to violence in and around schools.



CALL TO ACTION AREA 5: **Generate and use evidence**

Education data systems should track how technology is used or contributes to violence in and around schools. Monitoring should also cover vendors' compliance with safety and privacy standards.²⁰ Governments and partners should integrate technology-facilitated violence into school-based surveys and commission research to

identify effective strategies for preventing and responding to technology-facilitated violence, in and around and through schools. Evidence and lessons learned should be shared across the Safe to Learn coalition and with other stakeholders, including the tech industry, to drive innovation and continuous improvement.



Annex

Safe to Learn Benchmarks: integrating components on prevention and response to technology-facilitated violence²¹



CALL TO ACTION AREA 1: Implement laws and policies

BENCHMARK	HOW TO INTEGRATE PREVENTION AND RESPONSE TO TECHNOLOGY-FACILITATED VIOLENCE*
1.1: The national government includes prevention of violence in and around schools as a specific strategy in education sector policies, plans, and budgets.	■ Integrate technology-facilitated violence within violence prevention commitments in national policies and plans (in a technology ‘neutral’ manner). ■ Include assessment of how online violence impacts education sector objectives in Education Sector Analyses or annual sector and policy reviews.* ■ Introduce a framework policy setting out digital services and platforms that are approved for procurement and use in educational settings, with safety-by-design, privacy-by-default, and age-appropriate-design standards. ■ Require child-rights and data protection impact assessments (CRIAs/ DPIAs) for all school-endorsed platforms and publish a list of approved EdTech with minimum safety criteria.²²
1.2: There is explicit prohibition of corporal punishment in schools, and policies are in place to support positive discipline and classroom management.	■ Use contextual learning activities that explore the role of technology in children’s behaviour to support teacher development on positive discipline and classroom management.
1.3: The roles and responsibilities of the Ministry of Education in response and referral to incidents of violence are clearly set out in the multi-sectoral national child protection policy framework.	■ Integrate technology-facilitated violence into national, district, and school safeguarding policies and frameworks, with due consideration of children facing multiple forms of discrimination. This includes updating reporting and referral mechanisms to enable referrals to cybercrime units, helplines, hotlines, and platform escalation channels.

Note: The lines marked by an ‘*’ are those that are already included in the Safe to Learn Programmatic Framework under key interventions.



CALL TO ACTION AREA 2:

Strengthen prevention, risk mitigation and response in education systems and at the school level

BENCHMARK	HOW TO INTEGRATE PREVENTION AND RESPONSE TO TECHNOLOGY-FACILITATED VIOLENCE*
2.1: Key violence prevention strategies are embedded in curriculum-based activities for children.	■ Ensure that 'online' (and 'offline') violence is reflected in student curricula and teacher training related to violence prevention.* ■ Integrate digital literacy and safety into relevant curriculum. This should cover content such as respectful online behaviour, cyberbullying prevention, technology-facilitated gender-based violence, consent, image-sharing, scam awareness, and help-seeking.
2.2: Child safeguarding principles and procedures are in place in schools, inclusive of codes of conduct, and safe recruitment standards.	■ Integrate online safety into child safeguarding principles and procedures. This should include acceptable use, device and network management, classroom streaming and recording, data handling, and screening standards for roles with online access to children. ■ Ensure child-friendly reporting and support mechanisms, both online and in-person, are available and promoted widely. ■ Update teacher professional standards, codes of conduct and safeguarding guidance and training to cover digital settings (e.g., boundaries for one-to-one messaging, out-of-hours contact, classroom recording, and responsible AI tool use). ■ Train school personnel to handle disclosure and cases of online violence, as well as on how to work with children who are showing signs of psychological distress due to violence. ■ Support for teachers and school leaders to strengthen their digital literacy skills.* ■ Provide parents and caregivers with regular information on school use of technologies, online safety expectations, and safeguarding procedures.
2.3: Each school has at least one focal point who is capacitated to provide front-line mental health and psychosocial support to children experiencing violence.	■ Update training for school counsellors to include modules on technology-facilitated violence, crisis response and referral pathways, and establish agreements with external MHPSS providers specializing in online harm.
2.4: The physical environment in and around schools is safe and designed with the well-being of children in mind.	■ Integrate safe connectivity baselines (e.g., age-appropriate filtering) and privacy-preserving defaults for devices.

Note: The lines marked by an "*" are those that are already included in the Safe to Learn Programmatic Framework under key interventions.



CALL TO ACTION AREA 3:

Shift social and gender norms and promote behaviour change

BENCHMARK	HOW TO INTEGRATE PREVENTION AND RESPONSE TO TECHNOLOGY-FACILITATED VIOLENCE*
3.1: There is wide dissemination and engagement with stakeholders to build knowledge and appreciation of child rights and laws prohibiting violence.	■ Integrate children's rights in relation to the digital environment and online safety laws and standards, as well as reporting and support mechanisms, into stakeholder engagement initiatives at national, district, and school levels. ■ Build the capacity of parent-teacher associations and school management committees to incorporate both 'offline' and 'online' efforts to prevent and respond to violence into their concerns.*
3.2: Specific, evidence-informed interventions are researched and implemented, addressing social norms that drive key forms of violence and/or helping children manage risks.	■ Commission/endorse evidence-based programmes that address harmful social and gender norms driving violence, including technology-facilitated violence, and examine differentiated risk factors in digital environments. ■ Provide national policies or guidelines that give guidance on developing and implementing evidence-based interventions to address social norms surrounding key forms of violence, including digital safety.*
3.3: Young people, parents, teachers and community members in and around schools are engaged and active on the topic of school violence.	■ Integrate digital safety into contextualized communications and community engagement initiatives at national, district, and school levels, co-designed with children and young people. ■ Embed child-rights education that goes beyond awareness to develop children's practical understanding of rights and responsibilities in digital environments – covering privacy, consent, image-sharing, data protection, and respectful online communication. ■ Use national- or local-level data on the incidence, nature, impacts and costs of school violence, both 'online' and 'offline', to raise awareness among teachers, parents, policymakers, donors, the media and the public and to advocate for change.* ■ Promote learners' leadership and peer-to-peer initiatives that encourage positive online behaviours.

Note: The lines marked by an '*' are those that are already included in the Safe to Learn Programmatic Framework under key interventions.



CALL TO ACTION AREA 4: Invest resources effectively

BENCHMARK	HOW TO INTEGRATE PREVENTION AND RESPONSE TO TECHNOLOGY-FACILITATED VIOLENCE*
4.1: Domestic resources that have been allocated to support interventions and capacity building activities to prevent and respond to violence in schools.	■ Generate and use evidence on the costs of violence in and around schools, including 'online' violence, to advocate for greater and better public investment.* ■ Create national, sub-national and school budget lines to integrate digital dimensions into safeguarding (e.g., teacher continuing professional education, vendor audits) and financing safe connectivity. ■ Embed safety and privacy criteria into contracts for procurement and include requirements for independent audits of EdTech and other relevant providers.
4.2: Development partners provide resources targeting national or subnational level to end violence in schools, investing in effective approaches.	■ Leverage development partner resources for integrating online safety into prevention and response to violence in schools.
4.3: There is private sector engagement in the provision of financial and non-financial resources including technical support, expertise and advocacy towards ending violence in schools.	■ Generate and use evidence on the costs of violence in schools to advocate for greater and better private sector investment in violence prevention and response in and through schools, including 'online' violence.* ■ Broker partnerships with relevant companies to enable safe connectivity and device management as well as broader efforts to address technology-facilitated violence in and around schools.²³ ■ Advocate for greater transparency, accountability, and responsibility from the private sector, while urging governments to oversee business conduct, services and design to proactively tackle bullying and harassment and other technology-facilitated violence.

Note: The lines marked by an "*" are those that are already included in the Safe to Learn Programmatic Framework under key interventions.



CALL TO ACTION AREA 5: Generate and use evidence

BENCHMARK	HOW TO INTEGRATE PREVENTION AND RESPONSE TO TECHNOLOGY-FACILITATED VIOLENCE*
5.1: Information and reporting of incidents allow for disaggregated baseline information and monitoring of trends that reflect needs and gaps in the system.	■ Tag incident records with a ‘digital’ identifier to track how technology is used or contributes to violence in and around schools. ■ Monitor EdTech providers’ compliance with safety and privacy standards and publish findings annually.
5.2: There is regular data collection on prevalence and forms of violence in schools using methods that follow high ethical standards.	■ Integrate technology-facilitated violence into school-based survey programmes.
5.3: Decisions on replication and scale-up of violence prevention initiatives are based on evaluations of trailed models and approaches.	■ Commission impact and process evaluations of digital safety programmes and share learnings to inform replication and scale-up. ■ Share evidence and lessons learned with Safe to Learn partners, government stakeholders, and the technology industry to promote innovation and continuous improvement in preventing and responding to technology-facilitated violence.

Note: The lines marked by an “*” are those that are already included in the Safe to Learn Programmatic Framework under key interventions.



Key references

Safe to Learn, [Safe to Learn Call to Action](#), 2023.

Safe to Learn, [Global Programmatic Framework and Benchmarking Tool](#), 2021.

Safe to learn, [Diagnostic tool](#), Safe to Learn, 2021.

United Nations Children's Fund, [Child Protection in Digital Education: Policy Brief](#), UNICEF, New York, January 2023.

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

UN Committee on the Rights of the Child, [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), UN Doc CRC/C/GC/25, 2 March 2021.

Additional references

London School of Economics, Digital Futures for Children, [EdTech findings from the DFC – EdTech matters for children's learning, privacy and other rights](#), accessed March 2026.

United Nations Educational, Scientific and Cultural Organization, [AI Competency Framework for Students](#), UNESCO, Paris, 2024.

United Nations Educational, Scientific and Cultural Organization, [AI Competency Framework for Teachers](#), UNESCO, Paris, 2024.

United Nations Educational, Scientific and Cultural Organization, [Guidance for Generative AI in Education and Research](#), UNESCO, Paris, 2023.

United Nations Educational, Scientific and Cultural Organization, [ICT Competency Framework for Teachers](#), 3rd ed., UNESCO, 2018.

United Nations Educational, Scientific and Cultural Organization, [Recommendation on Education for Peace, Human Rights and Sustainable Development](#), 42nd UNESCO General Conference, UNESCO, November 2023.

United Nations Educational, Scientific and Cultural Organization, [Recommendation on the Ethics of Artificial Intelligence](#), UNESCO, 2022.

United Nations Population Fund, United Nations Children's Fund and Save the Children, [Technology-Facilitated Gender-Based Violence: Considerations across the life course](#), 2025.

United Nations Children's Fund, [Artificial Intelligence and Child Sexual Abuse and Exploitation](#), UNICEF, 2026.

United Nations Children's Fund, [Assessing Child Rights Impacts in Relation to the Digital Environment: Implementing the D-CRIA Toolbox](#), UNICEF, 2025.

United Nations Children's Fund, [Digital Education Strategy 2025–2030: Beyond digital as usual – An equity-driven, human-centered digital and AI strategy for learning](#), UNICEF, 2026.

United Nations Children's Fund, [Policy Brief: Protecting Children from Violence and Exploitation in Relation to the Digital Environment](#), UNICEF, 2024.

United Nations Children's Fund Innocenti – Global Office of Research and Foresight, [Data Governance for EdTech: Policy Recommendations](#), UNICEF Innocenti, Florence, 2025.

United Nations Children's Fund Innocenti – Global Office of Research and Foresight, [Guidance on AI and Children](#), 3rd ed., UNICEF Innocenti, Florence, 2025.

United Nations Children's Fund Innocenti – Global Office of Research and Foresight, [Disrupting Harm Project: Generating high-quality evidence on technology-facilitated sexual exploitation and abuse of children](#), UNICEF Innocenti, <<https://www.unicef.org/innocenti/projects/disrupting-harm>>, accessed March 2026.

United Nations Children's Fund Innocenti – Global Office of Research and Foresight, [Good Governance of Children's Data Project: Developing innovative pathways to improve the governance of children's data](#), UNICEF Innocenti, <<https://www.unicef.org/innocenti/projects/good-governance-childrens-data>>, accessed March 2026.

United Nations Children's Fund, Ministry of Foreign Affairs of Finland, Arm and Asian Development Bank, The EdTech for Good Framework, < <https://www.unicef.org/digitaleducation/edtech-for-good>>, accessed March 2026.

United Nations Children's Fund, Ministry of Foreign Affairs of Finland, Arm and Asian Development Bank, The Learning Cabinet, < <https://www.unicef.org/innovation/simplifying-edtech-discover-learning-cabinet>>, accessed March 2026.

United Nations Children's Fund, [Measuring Technology-Facilitated Violence against Children in Line with the International Classification of Violence against Children](#), UNICEF, New York, 2025.

United Nations Children's Fund and United Nations Human Rights Office of the High Commissioner, [Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment: A contribution to the B-Tech project](#), 2024.

United Nations General Assembly, [Rights of the Child](#), UN Doc A/RES/78/187, 22 December 2023.

United Nations Human Rights Council, [Safety of the Child in the Digital Environment](#), UN Doc A/HRC/RES/56/6, 10 July 2024.

United Nations Human Rights Council, [The Right to Be Safe in Education: Report of the Special Rapporteur on the right to education – Advance edited version](#), UN Doc A/HRC/59/41, 27 May 2025.

Endnotes

- 1 Safe to Learn, Call to Action (2023); Safe to Learn, Global Programmatic Framework and Benchmarking Tool (2021); Safe to Learn, Call to Action (2023) Safe to Learn, Diagnostic Tool (2021); Safe to Learn, Global Programmatic Framework and Benchmarking Tool (2021).
- 2 Insights from this note will be used to enhance the forthcoming edition of the STL Technical Package.
- 3 This Note refers to digital, rather than online, as more expansive. This aligns with the Committee on the Rights of the Child, General Comment #25, paragraph 2: 'The digital environment is constantly evolving and expanding, encompassing information and communications technologies, including digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology.'
- 4 OECD, 'Children in the digital environment: Revised typology of risks', OECD Digital Economy Papers, No. 302, OECD Publishing, Paris, 2021. Available at: <https://doi.org/10.1787/9b8f222e-en>.
- 5 United Nations Children's Fund, 'Child Protection in Digital Education: Policy Brief', UNICEF, New York, January 2023. Available at: <http://www.unicef.org/documents/child-protection-digital-education>. See, for example, 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. Available at: <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments>.
- 6 'Nudify' or 'undress' apps are AI apps that appear to remove clothing from photos turning 'everyday' images into sexually explicit images. See, for example, United Nations Children's Fund, Artificial Intelligence and Child Sexual Abuse and Exploitation, UNICEF, February 2026. Available at: <https://www.unicef.org/reports/artificial-intelligence-and-child-sexual-abuse-and-exploitation>; eSafety Commissioner (Australia), 'Deepfake damage in schools: How AI-generated abuse is disrupting students, families and school communities', 27 June 2025. Available at: <https://www.esafety.gov.au/newsroom/blogs/deepfake-damage-in-schools-how-ai-generated-abuse-is-disrupting-students-families-and-school-communities>. See also: Internet Watch Foundation and CEOP Education (UK), 'Child sexual abuse material generated by artificial intelligence: An essential guide for professionals who work with children and young people', Internet Watch Foundation, 2025. Available at: <https://www.iwf.org.uk/media/ceel0u4z/ai-guidance-england-final.pdf>; Grossman, S., Pfefferkorn, R., & Liu, S, 'AI-Generated Child Sexual Abuse Material: Insights from Educators, Platforms, Law Enforcement, Legislators, and Victims', Version 1, Stanford Digital Repository, 2025. Available at: <https://doi.org/10.25740/mn692xc5736>.
- 7 See: Bogotá Call to Action, Global Ministerial Conference on Ending Violence against Children, November 2024. Available at: <https://endviolenceagainstchildrenconference.org/call-to-action/>.
- 8 United Nations Children's Fund, Digital Education Strategy 2025-2030, Beyond digital as usual: An equity-driven, human-centered digital and AI strategy for learning (2026). Available at: <https://www.unicef.org/digitaleducation/reports/unicef-digital-education-strategy-2025-2030>
- 9 World Health Organization, INSPIRE: Seven strategies for ending violence against children, WHO, Geneva, 2016. Available at: <https://www.who.int/publications/i/item/9789241565356>.
- 10 UN Committee on the Rights of the Child (2021). General comment No. 25 on children's rights in relation to the digital environment. UN Doc CRC/C/GC/25; UN Human Rights Council (2025). The Right to Be Safe in Education: Report of the Special Rapporteur on the right to education. UN Doc A/HRC/59/41; UN Human Rights Council (2024). Safety of the Child in the Digital Environment. UN Doc A/HRC/RES/56/6; UN General Assembly (2023). Rights of the Child in the Digital Environment. UN Doc A/RES/78/187; UNESCO (2023). Recommendation on Education for Peace, Human Rights and Sustainable Development. 42nd Session, Paris.
- 11 See further: United Nations Children's Fund, 'Data brief on Measuring Technology-facilitated Violence against Children in line with the International Classification of Violence against Children', UNICEF, New York, March 2025. Available at: <https://data.unicef.org/resources/data-brief-on-measuring-technology-facilitated-violence-against-children-in-line-with-the-international-classification-of-violence-against-children-icvac/>. On technology-facilitated child sexual abuse and exploitation, see: Interagency Working Group, 'Terminology guidelines for the protection of children from sexual exploitation and sexual abuse', Second edition, ECPAT International, 2025. Available at: <https://ecpat.org/wp-content/uploads/2025/04/Second-Edition-Terminology-Guidelines-final.pdf>.
- 12 United Nations Children's Fund, 'Protecting children from violence and exploitation in relation to the digital environment: Policy Brief', UNICEF, New York, October 2024, p. 7. Available at: <https://www.unicef.org/documents/protecting-children-violence-and-exploitation-relation-digital-environment>

- 13 <https://www.ungei.org/publication/whole-school-approach-prevent-school-related-gender-based-violence>
- 14 Child rights due diligence includes child rights impact assessments. See further: United Nations Children's Fund, Assessing child rights impacts in relation to the digital environment – Implementing the D-CRIA Toolbox. Available at: <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA>
- 15 The EdTech for Good Framework. Available at: <https://www.learningcabinet.org/edtech-for-good-framework/>; UNICEF Innocenti – Global Office of Research and Foresight, 'Data Governance for EdTech: Policy Recommendations', UNICEF Innocenti, Florence, September, 2025. Available at: <https://www.unicef.org/innocenti/reports/data-governance-edtech>
- 16 See further: UN Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, UN Doc CRC/C/GC/25, 2 March 2021, paras 104-5.
- 17 This includes comprehensive sexuality education in line with international guidance: United Nations Educational, Scientific and Cultural Organization, Joint United Nations Programme on HIV/AIDS, United Nations Population Fund, United Nations Children's Fund, United Nations Entity for Gender Equality and the Empowerment of Women, & World Health Organization. (2018). International Technical Guidance on Sexuality Education: An evidence-informed approach. UNESCO, Paris. Available at: <https://www.unesco.org/en/articles/international-technical-guidance-sexuality-education-evidence-informed-approach>.
- 18 UNICEF Innocenti – Global Office of Research and Foresight, Who perpetrates online child sexual exploitation and abuse? Disrupting Harm Data Insight 8, Safe Online. End Violence Partnership, UNICEF, 2023. Available at: <https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf>.
- 19 UN Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, UN Doc CRC/C/GC/25, 2 March 2021, para 103. <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>
- 20 This includes national standards and the EdTech for Good Framework, a global asset that can be adapted across different national contexts. Available at: <https://www.learningcabinet.org/edtech-for-good-framework/>
- 21 The benchmarks in this document are based on the original Safe to Learn *Global Programmatic Framework and Benchmarking Tool* [2021]. They do not incorporate revisions to benchmarks introduced in the 2023 refreshed *Call to Action*, as these technical resources were developed prior to the refreshed Call to Action release.
- 22 The Learning Cabinet is a global platform, co-hosted by UNICEF, that lists EdTech solutions screened against the EdTech for Good Framework criteria. <https://www.learningcabinet.org/>
- 23 For instance, companies that work in Ed Tech and IT.



 **Safe to Learn** | unicef  | for every child