EdTech Hub

Clear evidence, better decisions, more learning.

POSITION PAPER

EdTech Horizon Scan

Rapid scan of online safety in education

Date November 2022

Authors Haani Mazari
Tom Kaye

DOI 10.53832/edtechhub.0136

UKaid from the British people

THE WORLD BANK

unicef for every child

#EdTechHub @GlobalEdTechHub edtechhub.org

About this document

Recommended citation

Mazari, H., & Kaye, T. (2022). *EdTech Horizon Scan: Rapid scan of online safety in education*. Position paper. https://doi.org/10.53832/edtechhub.0136 Available at https://docs.edtechhub.org/lib/3QBCENK5 . Available under Creative Commons Attribution 4.0 International, https://creativecommons.org/licenses/by/4.0/. Available under Creative Commons Attribution 4.0 International.

Notes

EdTech Hub is supported by UK aid (Foreign, Commonwealth and Development Office), Bill & Melinda Gates Foundation, World Bank, and UNICEF. The views expressed in this document do not necessarily reflect the views of UK aid (Foreign, Commonwealth and Development Office), Bill & Melinda Gates Foundation, World Bank, and UNICEF.

Reviewers

Laila Friese and Maria Tubio

Contents

1. Introduction

EdTech Hub horizon scans are publications designed to provoke thinking on a range of topics related to the design, implementation, oversight, and monitoring and evaluation of educational technology (EdTech) tools, products, services, and related ideas.

The scans DO contain a range of sources that have been identified by the authors as interesting and insightful. These have been synthesised to foster ongoing conversations as the EdTech field rapidly evolves. These scans ARE NOT designed to be comprehensive and should not be confused with systematic literature reviews or academic literature. They are quick guides that are part of the Hub's commitment to sharing knowledge fast and learning out loud. Should you have any questions or feedback on this horizon scan, we would love for you to contact us here.

This EdTech Horizon Scan examines the issue of online safety in digital education — why it should be prioritised, how it is currently being approached, and its potential to become central to education design in low- and middle-income countries. Given that the internet has no borders, there is much to be done to address online safety in all parts of the world — high-income and low- and middle-income countries alike.

2. What is online safety and why is it important?

While digital education has the potential to improve learning outcomes for some of the most marginalised, it also runs the risk of exposing vulnerable young people to inappropriate content and potentially dangerous situations. Although one in three internet users worldwide is a child, the internet was designed for adults and not enough has been done to reframe this reality (↑ITU, 2020a). Children and young people often navigate digital spaces with far more skill and understanding than their parents and are exposed to a much larger array of sites, content, and people. But digital fluency does not arm children with the skills, awareness, and responsiveness required to protect themselves socially, psychologically, and physically.

Being safe online means individuals protecting themselves and others from harm and risks they could be exposed to when accessing the internet through any device. Although knowledge of online safety is important for all individuals, children and young people are particularly vulnerable to online harms. One of the most pernicious dangers young people can face on the internet is sexual exploitation and abuse, which can be experienced virtually or with digital technology as a facilitator of grooming for in-person abuse (↑ITU, 2020a; ↑UNICEF, 2011). But children and young people can also suffer from serious social and psychological harm that could result from engaging with inappropriate content or face reputational damage from sharing personal content (↑ITU, 2020a; ↑UNICEF, 2011.) To ensure children are able to use technology safely to enhance their learning, explore their creativity, and further their development they require some scaffolding to safeguard their digital participation (↑UNICEF, 2011).

Even in high-income countries like the United Kingdom, parents increasingly believe that the risks of their children being online outweigh the benefits (↑Ofcom, 2019). Parental and community attitudes towards technology have been noted to stifle EdTech usage in many contexts, where parents are torn between allowing their children to use technology to access learning and reducing the safety risks associated with technology use (see for example ↑Gür & Türel, 2022). In low- and middle-income countries, concerns about online safety can have a greater impact along the lines of gender, where girls are likely to have limited access to using the internet and digital media due to caregiver attitudes (↑Allier-Gagneur & Moss Coflan, 2020). In this sense, cultivating the boundaries, awareness, and responsiveness required to

navigate the digital space safely could potentially help improve equitable access to technology-enhanced education in low- and middle-income countries.

3. How can we protect children online?

Building a safer digital space requires support and collaboration at the national and international level, between and across governments, non-profit organisations, academics, tech companies, and tech users. While cross-sectoral collaborations have helped bolster safeguarding legislation, policies, and mechanisms, adults from communities must be engaged to protect children online.

3.1 What is currently being done to protect children online?

Many governments have applied digital scaffolding by introducing legislation, strengthening policies, and creating channels to ban inappropriate content and prosecute offenders (↑UNICEF, 2011). Transnationally, WePROTECT Global Alliance[1] and the Global Partnership and Fund to End Violence against Children[2] are among some of the organisations that help countries develop coordinated responses to tackle online child sexual exploitation. However, of the countries with digital legislation in place, many have not yet updated legislation to address online harms beyond cyber security and data protection. High-income countries are beginning to introduce more specific policies regarding digital engagement (for example, the United Kingdom's Online Safety Bill[3] and Australia's Online Safety Act).[4] These policies aim to make social media companies more accountable for the online safety of their users. While legislation forms an essential part of the online safety response, it does not, however, sufficiently address online safety in terms of the creation and proliferation of child abuse images or criminalising grooming (↑UNICEF, 2011).

Digital legislation has been bolstered by emerging technologies that help locate abusers and identify and filter inappropriate content. At an international level, Interpol's artificial intelligence (AI) database uses image and video comparison software to make rapid connections between victims, abusers, and locations (↑ITU, 2020a). At the national level, some governments are attempting to block nationwide access to inappropriate or harmful content through keyword filters (↑UNICEF, 2011). Social media companies have responded to regulatory pressures by investing heavily in digital infrastructure (machine learning and AI detection) to detect inappropriate content. Despite these

[1] https://www.weprotect.org/ Retrieved 19 November 2022
[2] https://www.end-violence.org/ Retrieved 19 November 2022
[3] https://bills.parliament.uk/bills/3137 Retrieved 19 November 2022
[4] https://www.esafety.gov.au/whats-on/online-safety-act#:~:text=What%20is%20the%20Online%20Safety,harmful%20behaviour%20and%20toxic%20content. Retrieved 19 November 2022

mechanisms being fairly advanced, social media content removal also requires trust and safety personnel who navigate between policy and content to make safeguarding decisions. Furthermore, what qualifies as 'safe content' varies from context to context, where some governmental approaches are criticised as "undermining civil liberties (...) including the rights to privacy and free expression" (↑Ben-Hassine, 2019). This highlights the complexities of ensuring online safety while supporting meaningful digital participation.

While these mechanisms, policies, and procedures are essential to developing a protective digital environment, they must be brought to life through a whole systems approach, i.e., collaboration between the government, private sector, young people, and their parents (↑UNICEF, 2011; ↑Zubairi et al., 2022). For example, the World Economic Forum's Global Coalition for Digital Safety is accelerating public–private partnerships to tackle harmful and dangerous content through a community of engaged partners including Google, Microsoft, Amazon Web Services, Meta, Oxford Internet Institute, UNICEF, INTERPOL and several governments across the world (↑WEF, 2022). While governments and organisations have a responsibility to detect harmful behaviour to support online safety, adults within a child's community play a critical role in protecting children from the risks they face online.

3.2 What tools are available for families?

There is a range of tools that families and schools can use to filter and monitor a child's digital experience. Yet even in a high-income country like the United States, only 39% of parents report using parental controls to block, filter, or monitor their teenage child's online activities (↑Anderson, 2016). Considering that parents in high-income countries have greater awareness of online safety than parents in low- and middle-income countries, it is likely that parents in low- and middle-income countries would be less familiar with using parental controls.

3.2.1. Web and content filters (free)

Some level of basic filtering is available through all major web browsers including Microsoft Edge, Chrome, Firefox, Brave, and Opera. Many devices, including those made by Apple, Google, Huawei, Microsoft, and Samsung, have the option for parents to filter content and limit their child's screen time. Kaspersky Safe Kids[5] has a free version of its App that supports content filtration and screen usage limits. These filtering tools often use a variety of factors including content categories, keywords, IP addresses, and URLs /

[5] https://me-en.kaspersky.com/safe-kids Retrieved 19 November 2022

domains to block access to particular websites. However, some content filtration processes enforced by governments or used by parents can also be overridden through the use of Virtual Private Networks (VPNs) that can encrypt online traffic and disguise online identities.

3.2.2. Content monitoring (paid)

Payment-based content filters sometimes come with a range of features that can also monitor a child's activity. Types of monitoring tools range from recording device usage to identifying potential risks. Some tools push notifications with risk alerts if a child is exposed to content that is inappropriate. Other tools capture screenshots of digital activity, so parents can be aware of exactly how their child is using a device, while some go further and track a child's GPS coordinates to identify where they are.

3.2.3 Usage in low- and middle-income countries

With potentially less understanding of online safety and greater financial burden, most families in low- and middle-income countries cannot be expected to invest in expensive content monitoring tools that could range from USD 50 to USD 100 annually. They could, however, make use of easily available free content filtration tools that are available on the devices they already have. Furthermore, no filtration tool should ever be considered to be 100% effective, and thus it is critical to prioritise equipping communities with the awareness and skills to understand online safety.

3.3 What education and awareness programmes are available?

While a child's digital learning experience can be scaffolded through policies, legislation, and technology itself, teachers and caregivers must be equipped with awareness and skills to understand online safety (↑Kingsley, n.d; ↑UNICEF, 2011). There is evidence to indicate that of the parents with access to safeguarding technology, only just over 50% actually know how to activate it (↑UNICEF, 2011). As a result, rather than just considering the infrastructure that supports online safety, it is critical to consider how programmes work with communities to strive for the safety of children.

Below is a small number of examples of multinational and national organisations providing resources to support online safety in low- and middle-income countries. Many of these programmes have been developed through partnerships with experts in online safety or child protection. We have found that many of these programmes have been developed for high-income

countries but are now also being used (and sometimes localised) for low- and middle-income countries. These offer insights into the types of offerings in this area, but this list is neither exhaustive nor fully representative of all the resources and programmes available to parents, teachers, and children.

3.3.1. International Telecommunication Union (ITU)

The ITU (2020b) has developed 'Guidelines for parents and educators on Child Online Protection'. There are 13 areas of consideration for parents and 8 areas of consideration for educators. The document is available in English, Arabic, Chinese, French, and Russian. In English, the document is 58 pages long. These guidelines have been tailored to give advice or recommendations for different contexts because specific needs require individual consideration and because legal and cultural factors have an important bearing on how these guidelines might be used or interpreted in any given country or region. For a paraphrased version of the guidelines, see Figures 1 and 2 below:

Figure 1. *Paraphrased version of ITU's (2020) guidelines for parents on child online protection*

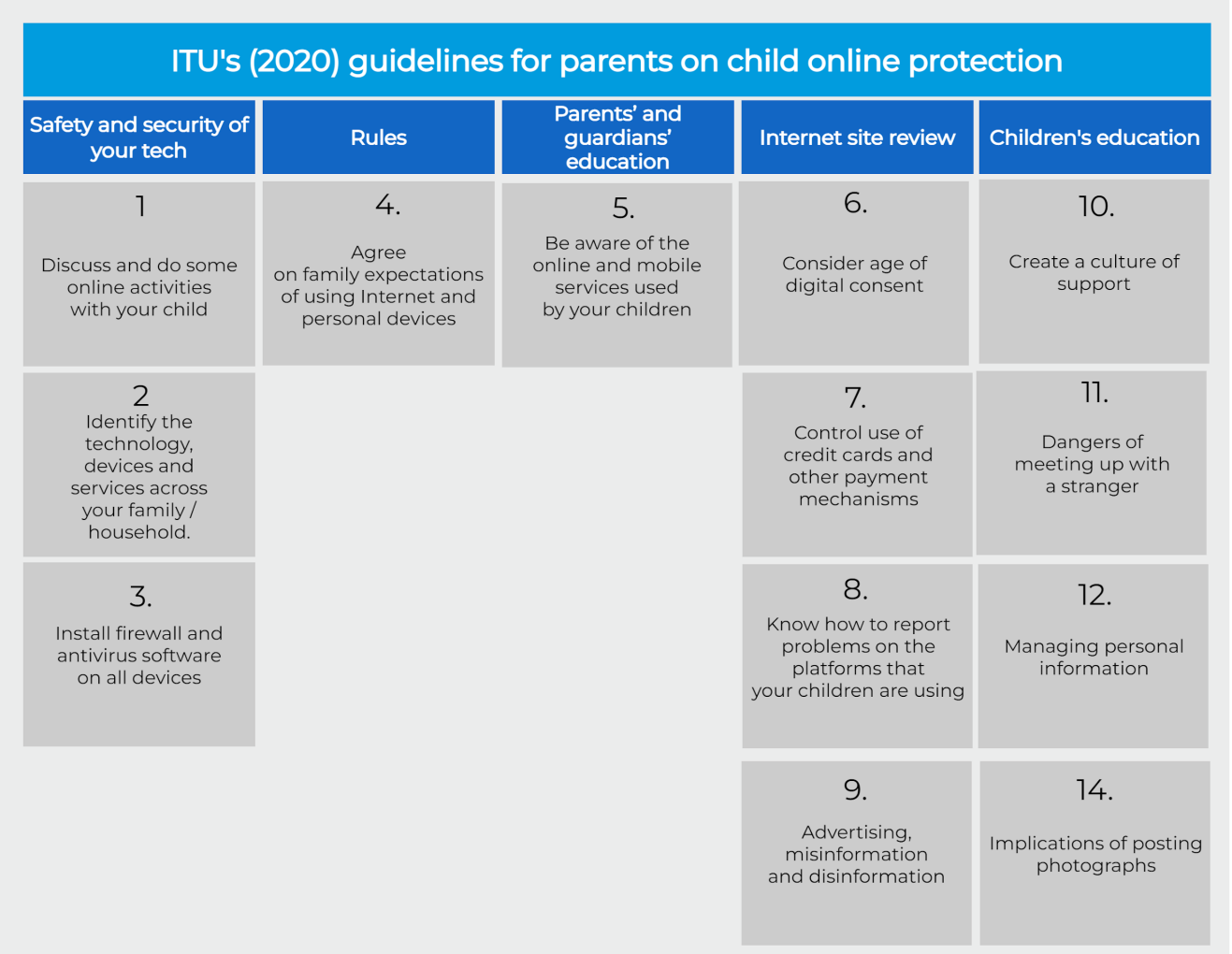
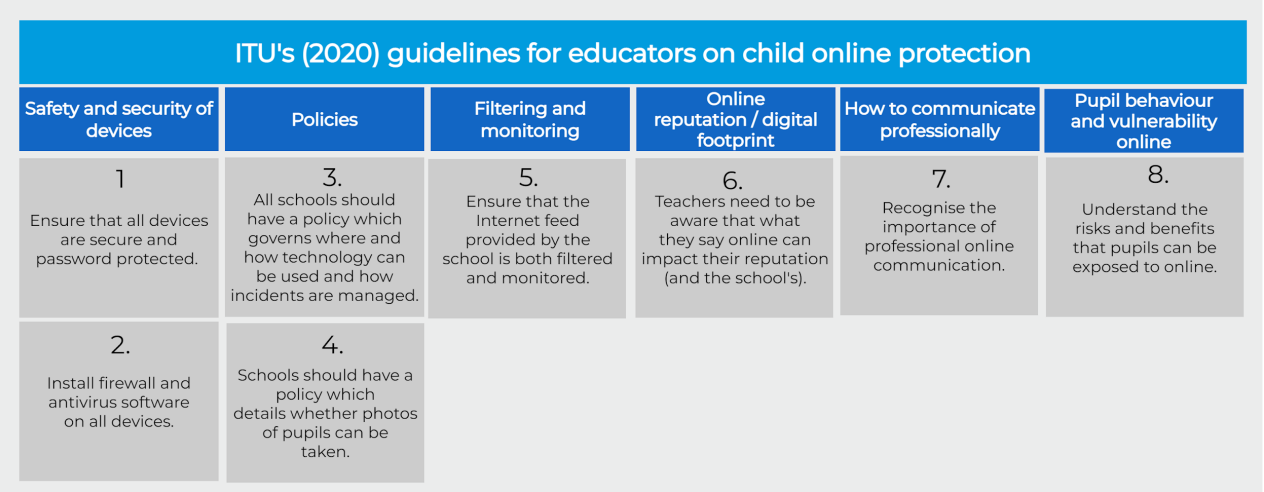


Figure 2. *Paraphrased version of ITU's (2020b) guidelines for educators on child online protection*



3.3.2. Google[6] (free)

Google has partnered with experts in digital safety (including iKeepSafe,[7] ConnectSafely[8] and Family Online Safety Institute)[9] to develop *Be Internet Awesome*,[10] which includes gamified lessons for children through 'Interland',[11] lesson plans and activity guides for teachers, and online safety guides and pledges for families. The programme was developed for use within the United States but is now being expanded internationally through partnerships. For example, in Bangladesh, Google has partnered with the non-governmental organisation BRAC, one of the largest global development entities, to launch Stay safe online.[12] *Be Internet Awesome* content is being culturally contextualised and translated into Bangla to reach over 16,000 students and 600 teachers from 125 schools across Bangladesh.

3.3.3. Meta[13] (free)

Meta has partnered with experts in child protection and online safety, including the Internet Watch Foundation,[14] the International Centre for Missing

[6] https://safety.google/families/ Retrieved 19 November 2022
[7] https://ikeepsafe.org/ Retrieved 19 November 2022
[8] https://www.connectsafely.org/?doing_wp_cron=1665761587.2110159397125244140625 Retrieved 19 November 2022
[9] https://www.fosi.org/ Retrieved 19 November 2022
[10] https://beinternetawesome.withgoogle.com/en_us/ Retrieved 19 November 2022
[11] https://beinternetawesome.withgoogle.com/en_us/interland Retrieved 19 November 2022
[12] https://www.banglanews24.com/english/national/news/bd/96152.details Retrieved 19 November 2022
[13] https://www.facebook.com/business/news/facebook-commitment-to-online-safety Retrieved 19 November 2022
[14] https://www.iwf.org.uk/ Retrieved 19 November 2022

and Exploited Children,[15] and Child Helpline International.[16] These partnerships have led to the development of step-by-step resources for teachers (My Digital World)[17] and textual resources for children and caregivers (We Think Digital),[18] and a portal called StopNCII (Stop Non-Consensual Intimate Image Abuse)[19] that aims to stop the sharing of non-consensual intimate images. Meta works with local partners in low- and middle-income countries to translate these tools. For example, the StopNCII portal has been translated into Urdu for use in Pakistan.

3.3.4. Terre des Hommes[20] (free)

Terre des Hommes has partnered with ChildLine Kenya and the African Institute for Child Studies to implement an online safety programme in Kenya. The programme has a multimedia approach that includes training manuals (a facilitator's guide and a student workbook) and seven animated stories. The animated videos for the training are available for free on YouTube.[21]

3.3.5. Child Online Africa[22] (free)

Africa Digital Leaders (ADL) is a hybrid fellowship programme that targets children between the ages of 8–6 to build their skills and capacity to use technology responsibly and safely.

3.3.6. MySocialLife[23] (paid)

MySocialLife offers a payment-based programme for online safety training to learners, parents, teachers, and school psychologists. Content for students is specified by their age group, with a different offering for high-school students and junior-school students. After watching a 75-minute training video, teachers use MySocialLife content to train students in the classroom. The programme covers eight modules including digital identity, cyberbullying and empathy, critical thinking, privacy settings, cyber security, mental health, sexuality online, and digital potential. Although this is a payment-based programme that has been developed for private schools, for every school that completes the

[15] https://www.icmec.org/ Retrieved 19 November 2022
[16] https://childhelplineinternational.org/ Retrieved 19 November 2022
[17] https://mydigitalworld.fb.com/mena/ Retrieved 19 November 2022
[18] https://wethinkdigital.fb.com/ Retrieved 19 November 2022
[19] https://stopncii.org/ Retrieved 19 November 2022
[20] https://www.terredeshommes.nl/en/publications/online-safety-for-children-training-module-kenya Retrieved 19 November 2022
[21] https://www.youtube.com/playlist?list=PLO8-ll5fzrwR9CsR2ZNrtqN-wtg21234Z Retrieved 19 November 2022
[22] https://www.childonlineafrica.org/africa-digital-leader Retrieved 19 November 2022
[23] https://www.mysocialife.com/ Retrieved 19 November 2022

programme, MySocialLife provides it free of charge to a school on the African continent that cannot afford it. However, the school would require internet connectivity and a screen to facilitate the programme.

3.3.7. National Online Safety[24] (freemium)

National Online Safety, a UK-based company, offers a freemium subscription model for online safety training. While programmes for educators and schools are available on an annual basis, their free programme includes one user account that can access a parents' course, as well as online safety guides on 12 topics, some of which include mental health, online bullying, online relationships, and social media. National Online Safety has partnered with safeguarding tool providers (i.e., Smoothwall[25]) to offer their training package to supplement safeguarding technology.

[24] https://nationalonlinesafety.com/ Retrieved 19 November 2022
[25] https://resources.smoothwall.com/ Retrieved 19 November 2022

4. What needs to be considered?

Many of the examples of online safety training shown above have been developed for high-income country contexts and have then been translated into local languages to cater to populations in low- and middle-income countries. But little can be done otherwise, as research on online safety has so far been undertaken mainly in high-income countries. This is because contemporary adults from low- and middle-income countries are less likely to have a grasp of the digital world and its challenges and opportunities (↑UNICEF, 2011). Lack of parental awareness and digital skills, difficult economic conditions, and underdeveloped regulatory frameworks can further exacerbate potential risks and the likelihood of harm (↑UNICEF, 2011).

To explore online safety in countries around the world, UNICEF Innocenti has partnered with the London School of Economic and Political Science (LSE) and the EU Kids Online network on Global Kids Online.[26] This project examines online opportunities and risks for children across eleven countries. All research tools developed are open source and are accompanied by guidance on how to contextualise the tool to support a cross-country comparative analysis. The following sections draw on the findings of ↑Livingstone et al.'s (2019) *Global Kids Online: Comparative Report* with some insights from conversations with implementers of online safety programmes. It highlights three areas that we believe require more of a focus to build knowledge about online safety, particularly in low- and middle-income countries, namely:

1. Online safety approaches
2. Online safety content
3. Building further evidence.

4.1 Online safety approaches

It is worth considering whether online safety programmes developed in line with the needs of high-income countries consider the diverse needs and experiences of communities in low- and middle-income countries. The type of technology children use, and where they use it, shape considerations for online safety programme design in low- and middle-income countries. For example, as ↑Livingstone et al. (2019, p. 21) point out —"While the first generation of internet users in the global North gained access via desktop computer, the pattern in the global South has been mobile first."

[26] http://globalkidsonline.net/ Retrieved 19 November 2022

Since mobile phones are the main access point to the internet for communities in low- and middle-income countries, parents and caregivers appear to play a more critical role in addressing online safety than educationists do. In most countries surveyed, less than half of children aged 9–17 years use the internet at school or college at least once a week. However, the level of support parents in low- and middle-income countries (for example, Ghana, the Philippines, and South Africa) provide to scaffold their child's internet use is significantly less than for parents in high-income countries (↑Livingstone et al., 2019).

These needs also shape the parents' role in supporting online safety. In countries with more restrictive parental support, the diversity of children's online activities appears to be reduced (↑Livingstone et al., 2019). Restrictive parental support can negatively impact the way children seek information and manage their digital privacy. Meanwhile, enabling approaches slightly improve children's digital skills while slightly reducing their exposure to online risks (↑Livingstone et al., 2019).

This scan has highlighted that while online safety has gained an increased focus in recent years, there is still much work to be done to ensure that approaches to online safety are relevant for all users. With use of the internet continuing to expand into new and different geographies and cultures on a daily basis, our approaches to online safety also need to adapt to ensure all children are equipped with the knowledge, skills, and attitudes they require to navigate the online world.

4.2 Online safety content

The topic of online safety itself is a sensitive one for different communities, with potential to trigger a range of parental responses varying from "panic to punishment" (↑Livingstone et al., 2019). Although many of the risks related to online safety are universal, consideration of cultural sensitivities could help mitigate the risk of decreased technology adoption.

In Bangladesh, where Google has partnered with BRAC to contextualise its *Be Internet Awesome* curriculum, BRAC has found a number of content-related issues that it is seeking to address to support effective engagement with communities. For example, a number of terminologies (e.g., 'sexting') are considered incongruent with community values, and are thus being adapted through careful cultural consideration prior to programme implementation. If left unaddressed, cultural incongruencies could run the risk of impacting the ways teachers and parents embrace technology for a child's learning. ↑Livingstone et al.'s (2019) research suggests that when internet use among children is not widespread, the discourse on its usage focuses on potential

harms rather than benefits. This raises the question of how online safety topics can be navigated without further restricting children's usage of the internet. Conversely, a spokesperson from MySocialLife feared that leaving critical topics unaddressed could potentially limit the awareness and information adults have to keep children safe. The balance between sensitive and effective online safety content is something that programme designers need to consider with some delicacy in their programming.

Similar to online safety approaches, online safety content needs to ensure that it is culturally and contextually relevant. For example, delivering education more broadly, ensuring that students are able to access online safety content means more than curating it from other contexts. Online safety proponents must ensure that content is adapted to suit both the delivery mechanisms and the cultural and linguistic contexts in which it is being deployed.

4.3 Building evidence

In general, more robust evaluations of the effectiveness of online safety programmes are increasingly required to provide better insights into whether and why these programmes are / are not having an impact on the safety of children.

Studies in high-income countries show that the greatest "risks to children are in the form of cyberbullying, exposure to inappropriate or illegal material, and sexual or other abuse either over the Internet or in person" (↑Trucano, 2009). However, we do not know enough about what poses the greatest risk to children in low- and middle-income countries. Without this information, online safety practices and training will be based on experiences from Europe and North America (↑Trucano, 2009). While partnerships between international and local organisations help contextualise online safety programming to make it more relevant and useful to communities, evidence gaps could potentially run the risk of online safety training not addressing topics that could be impacting the digital experiences of children in low- and middle-income countries.

Lacking context-specific evidence to inform design, online safety programmes in low- and middle-income countries require in-depth evaluation to support continuous improvements. For example, MySocialLife conducts a thorough evaluation of its programme at the school level. Their approach seeks to go beyond tracking the reach of their programme by evaluating how their content is being consumed, reacted to, and engaged with.

In order to ensure that digital content interventions are actually contributing to increased child safety online it is vital to collect more primary evidence that can provide insights into the effectiveness of these initiatives.

5. Summary

Children and young people often navigate digital spaces with far more skill and understanding than their parents. Children and young people have been exposed to a much larger array of sites, content, and people online and with greater intensity than their parents. But digital fluency does not arm children with the boundaries, awareness, and responsiveness required to protect themselves socially, psychologically, and physically.

Much is being done to scaffold children's digital experiences on the national and international level. While the mechanisms, policies, and procedures developed and strengthened by cross-sectoral partnerships are essential to developing a safe digital environment, they must be brought to life through a whole systems approach — collaboration between government, private sector, young people, and their parents (↑UNICEF, 2011; ↑Zubairi et al., 2022)

In this scan, we have explored a non-exhaustive list of programmes developed to equip parents, teachers, and children with online safety skills. Many of these programmes, however, were developed for high-income countries and are being adapted for use in low- and middle-income countries. We used findings from ↑Livingstone et al.'s (2019) Global Kids Online report to explore some considerations that must be made when addressing online safety in low- and middle-income countries. However, we do not have enough evidence currently about online safety in low- and middle-income countries to support context-specific programme design. Some good practices we have observed include a thorough localisation process supported by national partners to ensure content fits with cultural sensitivities and evaluation processes that support continuous improvement. Until more evidence is generated about the risks children in low- and middle-income countries encounter when navigating the digital world, it is critical that programme designers strengthen their approaches and content with community insights to ensure online safety programmes resonate with parents and teachers. Without cultural alignment, parental and community attitudes could potentially stifle EdTech usage, particularly for girls.

References

This bibliography is available digitally in our evidence library at https://docs.edtechhub.org/lib/3QBCENK5

Allier-Gagneur, Z., & Moss Coflan, C. (2020). *Your Questions Answered: Using Technology to Support Gender Equity, Social Inclusion and Out-Of-School Learning* (Helpdesk Response No. 14). EdTech Hub. https://doi.org/10.53832/edtechhub.0025. Available from https://docs.edtechhub.org/lib/VX7UW757. (details)

Anderson, M. (2016). Parents, Teens and Digital Monitoring. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2016/01/07/parents-teens-and-digital-monitoring/. (details)

Ben-Hassine, W. (2019). *Government Policy for the Internet Must Be Rights-Based and User-Centred | United Nations*. https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred. (details)

Gür, D., & Türel, Y. K. (2022). Parenting in the digital age: Attitudes, controls and limitations regarding children's use of ICT. *Computers & Education*, *183*, 104504. https://doi.org/10.1016/j.compedu.2022.104504. Available from https://www.sciencedirect.com/science/article/pii/S0360131522000756. (details)

ITU. (2020a) *Guidelines for Industry on Child Online Protection*. https://www.itu-cop-guidelines.com/industry.(details)

ITU. (2020b) *Guidelines for Parents and Educators on Child Online Protection*. https://www.itu-cop-guidelines.com/parentsandeducators.(details)

Kingsley, A. (n.d.). *Navigating the Shifting Sands of Online Safety*. GESS Education. Retrieved November 18, 2022, from http://www.gesseducation.com/gess-talks/articles/navigating-the-shifting-sands-of-online-safety. (details)

Livingstone, S., Kardefeld-Winther, D., & Saeed, M. (2019). *Global Kids Online: Comparative report*. (details)

Ofcom. (2019). *Children and parents: media use and attitudes report 2019*. 36. (details)

Trucano, M. (2009). *On-line safety for students in developing countries*. https://blogs.worldbank.org/edutech/online-safety-for-students. (details)

UNICEF. (2011). *Child Safety Online: Global challenges and strategies*. (details)

WEF. (2022). *Online safety: making the internet safer by tackling harmful content*. World Economic Forum. https://www.weforum.org/impact/online-safety/. (details)

Zubairi, A., Khalayleh, A., Baloch, I., Mazari, H., Kaye, T., & Groeneveld, C. (2022). *Pakistan Digital Learning Landscape Analysis* [Technical Report]. EdTech Hub. https://doi.org/10.53832/edtechhub.0093. Available from https://docs.edtechhub.org/lib/HEXCEXFK. Available under Creative Commons Attribution 4.0 International. (details)