United Nations
Educational, Scientific and
Cultural Organization

UNESCO Chair in
ICT for Development
Royal Holloway, University of London

Guidance Note 13
Ensuring that children are safe when using digital technologies for learning

From the Report: Education for the most marginalised post-COVID-19: Guidance for governments on the use of digital technologies in education

ACT THREE (OF THREE): GUIDANCE NOTES

Date	**November 2020**
Authors	**Tim Unwin** **Azra Naseem** **Alicja Pawluczuk** **Mohamed Shareef** **Paul Spiesberger** **Paul West** **Christopher Yoo**
Report homepage	**https://edtechhub.org/education-for-the-most-marginalised-post-covid-19/**

EdTech Hub
Clear evidence, better decisions, more learning.

Guidance Note: Ensuring that children are safe when using digital technologies for learning[1]

Context

Digital technologies are all too often seen as bringing nothing but positive benefits. As this Report has emphasised throughout, though, this is a dangerous myth, and for any benefits to be achieved by the use of digital technologies in education it is essential for governments to put in place measures to mitigate the harms that they can be caused through their use. Such harms are both intentional and unintentional. Moreover, what is seen in one culture as a benefit, may be seen in another as a harm. There is thus rather little international agreement on what should or should not be permitted on the Internet, on how this should be managed or policed, and who should be responsible for this. However, the one area that most jurisdictions and governments can agree on is that children should not be harmed through their use of digital technologies in general, and the internet in particular. This is therefore one area where positive international collaboration can be encouraged and built upon.

Children and young people are disproportionately affected by the threats of the digital world. Potential harms, including hate speech, online pornography, sexual abuse and harassment, bullying, and other forms of unwanted behaviour are far greater than is usually imagined. In 2019, for example, the UK-based internet Watch Foundation, registered an increase of 28% over the previous year in the number of Reports it confirmed as containing images and videos of child sexual abuse.[2] Almost a third of all webpages actioned by their analysts contained self-generated images, and three-quarters of these showed a girl aged 11–13; 89% of hosting sites were in Europe (including Russia and Turkey). Yet, according to INHOPE (leading the fight against child sexual abuse material) only 42 countries currently have a hotline within their network for reporting child sexual abuse material (CSAM); African and Asian countries are noticeable by their absence from this network. Additional risks include those associated with children's lack of privacy, disinformation, unwarranted data collection and algorithmic analysis of their digital behaviours. There is limited guidance on how children's data should be handled and protected against any unauthorised or unethical future use. Governments should aim to establish and follow a localised, responsive and future-proof child-centred ethical code of practice and companies need to co-operate with them to protect children's privacy and safety.

Access to digital technologies within education systems is one of the main ways through which children both access and also make themselves vulnerable to those seeking to exploit and abuse them through digital technologies. Governments must therefore ensure that they do everything that they can to limit such opportunities, train young people in the safe use of digital technologies, and prosecute those who seek to harm them through its use. Fortunately, there is now an increasing amount of wise advice

[1] Lead authors Azra Naseem, Alicja Pawlucsuk, and Tim Unwin.

[2] Internet Watch Foundation https://www.iwf.org.uk/sites/default/files/inline-files/Briefing%20-%20IWF%20Annual%20Report%202019.pdf.

for governments in how to address these issues. UNICEF's seminal report in 2017 thus highlights that there are three main forms of risk (content, contact and conduct) and that these intersect with three main types of harm (aggression and violence, sexual abuse, and commercial exploitation). They also note that the most vulnerable children tend to be those who are already most marginalised, girls, those from poorer households, those living in communities with a limited understanding of different forms of sexual abuse and child exploitation, those who have disabilities, those out of school, those with mental health problems, and those from other marginalised groups.

Furthermore, the Broadband Commission in 2019 reached consensus amongst its private sector and government partners on five key elements of a universal declaration to affirm their commitment to protect children as they access the internet. To achieve this goal, and to highlight their responsibility in educating all children for the digital future ahead of them, they asserted that they should:

- '**Proactively** utilise available and develop new innovative technologies to block child sexual abuse material and prevent networks and services, as well as the internal IT environment from being used by offenders to commit violations against children.
- **Design** age-appropriate digital services that best meet the needs of children while equipping them to protect themselves online.
- **Work** collectively, across policy, regulatory, the private sector, law enforcement, and national security circles to minimise the risk of violence, abuse, and exploitation of children online.
- **Protect** children's privacy, security and safety.
- **Challenge** existing policies, approaches, mindsets, technology tools, and any medium that knowingly or unknowingly hinder the cause of protecting children, building upon internationally recognised legal recommendations.'[3]

Guidance

This guidance identifies the most important first steps that governments need to take to ensure that children can use digital technologies safely to enhance their learning:

1. **The highest priority of governments must be to ensure that all children are provided with appropriate and ongoing training in the safe and acceptable use of digital technologies** before they are introduced to its use in education and learning.
2. Governments must **enact appropriate legislation to prevent the use of digital technologies for the exploitation of children**, and ensure that the police service and other agencies identify perpetrators and bring them to justice.
3. **Governments should ensure that they have mechanisms in place to facilitate international collaboration in child online safety**, both to ensure that good practices are shared and to bring perpetrators of crimes to justice.

[3] Broadband Commission/ITU (2019) *Child online safety universal declaration*, Geneva: ITU, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf.

4. Governments should ensure that there is a **national hotline for reporting all child sexual abuse material** (CSAM), and that this is integrated within the INHOPE international network.
5. **National education policies should mandate ministries and schools to provide digital safety training to all those involved in the national education system** (officials, administrators, head teachers, teachers, other educational facilitators, learners and parents) **on how to identify child online abuse, how to report it swiftly and in confidence, and how to support those encountering it.**
6. **Safe spaces should be created in all schools and educational institutions** where those suffering from online abuse can escape from digital technologies, learn safely through other means, and gain the skills necessary to participate actively as survivors in digital environments.
7. **Governments should fund media campaigns (TV, radio, social media) in local languages to highlight the issues surrounding child online safety, and how to protect them from harm.** These should aim to create a culture of support for children and their families, and remove the stigma attached to reporting online exploitation and bullying.

Examples

The following examples illustrate interesting initiatives in digital child safety, especially by governments:

- Australia, eSafety Commissioner (2019) *Safety by design overview*, Canberra: eSafety Commissioner, https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf.
- Broadband Commission/ITU (2019) *Child online safety universal declaration*, Geneva: ITU, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf.
- INHOPE hotlines, https://www.inhope.org.
- ITU (2020) *Guidelines on child online protection*, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP-2020-Guidelines.aspx, including specific guidance for policy makers in multiple languages https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.POL_MAKERS-2020-PDF-E.pdf.
- UK Council for Child Internet Safety (UKCCIS), https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.
- WeProtect Global Alliance (2018) *Working examples of model national response Capabiliti4es and implementation*, https://www.end-violence.org/sites/default/files/paragraphs/download/WePROTECT%20Global%20Alliance.pdf.

Suggested further reading

- Alder, R. (2015) 20 tips for creating a safe learning environment, *Edutopia*, https://www.edutopia.org/blog/20-tips-create-safe-learning-environment-rebecca-alber.
- DQ Institute (2020) *Child online safety index*, https://www.dqinstitute.org/child-online-safety-index/.

- ECPAT International and Religions for Peace (2016) *Protecting children from online sexual exploitation: A guide to action for religious leaders and communities*, New York: ECPAT International, Religions for Peace, UNICEF, https://www.unicef.org/protection/files/FBO_Guide_for_Religious_Leaders_and_Communities_ENG.pdf.
- Internet Watch Foundation (2019) *Annual report*, https://www.iwf.org.uk/report/iwf-2019-annual-report-zero-tolerance.
- The Children's Society and Young Minds (2018) *Safety net: Cyberbullying's impact on young people's mental health: Inquiry report,* London: The Children's Society and Young Minds, https://www.alexchalk.com/sites/www.alexchalk.com/files/2018-04/pcr144b_social_media_cyberbullying_inquiry_full_report.pdf.
- UNICEF (2017) *The state of the world's children 2017: Children in a digital world*, New York: UNICEF, https://www.unicef.org/publications/index_101992.html.

Any part of this document may be reproduced without permission, but with attribution to the EdTech Hub (https://edtechhub.org) and the authors. Please use this attribution statement when referencing this work:

> *Guidance Note: Ensuring that children are safe when using digital technologies for learning, by Azra Naseem, Alicja Pawlucsuk, and Tim Unwin is licensed under the Creative Commons Attribution 4.0 International License, except where otherwise noted.*

This guidance note is based on existing good practices, and advice received from participants in our consultations. Please feel free to use and share this information, but kindly respect the copyright of all included works and also share any adapted versions of this work.

United Nations
Educational, Scientific and
Cultural Organization

UNESCO Chair in
ICT for Development
Royal Holloway, University of London

EdTech Hub

Clear evidence, better decisions, more learning.

Publication typesetting by User Design,
Illustration and Typesetting
www.userdesignillustrationandtypesetting.com