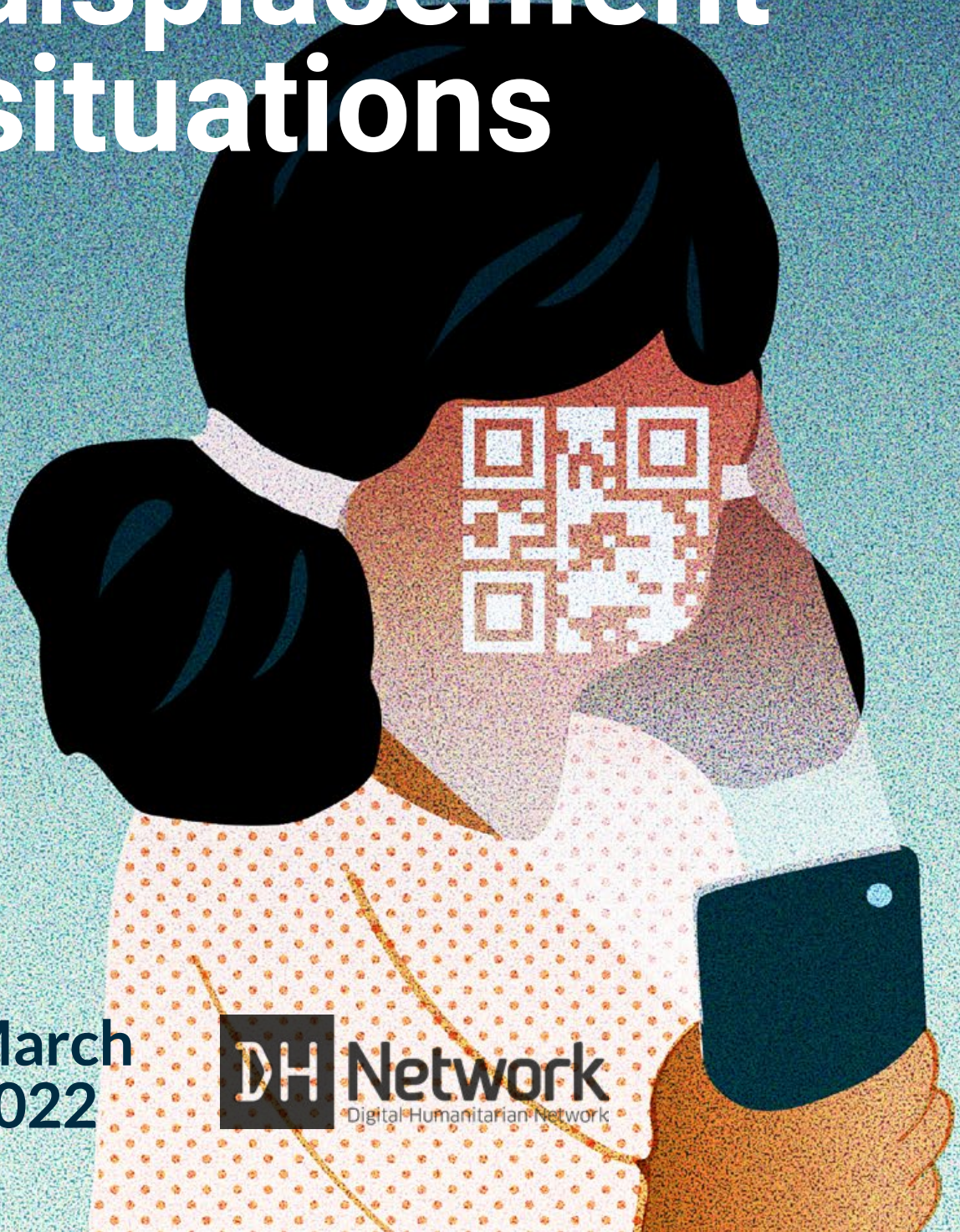
Mitigating physical risk posed by (education) technology:

To children in displacement situations



March 2022

DH Network
Digital Humanitarian Network

Licensing Information

Mitigating physical risk posed by (education) technology: **To children in displacement situations**

By

Dijie (Sariel) Lei (dijie.lei@gmail.com | Linkedin)
Master of Global Affairs, Munk School of Global Affairs and Public Policy, University of Toronto

Andrej Verity (verity@un.org | @andrejverity | LinkedIn)
United Nations Office for the Coordination of Humanitarian Affairs (UN-OCHA)

Design

Alexandra Sternin | alexsternin.com

This document was made possible with the support of

OCHA

Table of Contents

Acknowledgements

We would like to express our gratitude to those who shared their experience and expertise generously in the use of Education technology amongst displaced children. Without their contribution, this report would not be possible.

Name	Organization	Title
Stuart Campo	UNOCHA	Team Lead, Data Responsibility at the Centre for Humanitarian Data
Lynda Kigera	Norwegian Refugee Council	Global Roving EdTech Advisor

Introduction

Humanitarian agencies are increasingly leveraging technologies in their education programmes for displaced children. At the same time, existing data and reports suggest that such technologies, including Education Technology (Ed-tech), may introduce risks and potential physical harm to the vulnerable children. With more agencies becoming creative and innovative with education technologies, discussions on how to address the increasing risks are paramount.

This paper aims to introduce the types of potential risks an Ed-tech could impose for displaced children - with a specific focus on devices and data. Planning an effective intervention with digital devices requires thorough consideration about the specific context to rule out potential negative impacts from social and family structures, management of devices and digital exclusion. Data security requires all actors to collaborate and build a strong network for information management that rests on concrete ethical and legal standards. This work cannot be done alone. Organizations will need to work collaboratively with other responsible actors - including governments and multinational organizations - to develop relevant safeguarding frameworks and implement best practices.

Device

In the discourse about displaced children in today's age, making use of digital solutions or distributing devices becomes one of the top intervention suggestions. Therefore, understanding whether these children have restrained or unrestrained access to devices and wi-fi and to what level of confidentiality is incorporated are both crucial in planning for a safe and successful education intervention.

Risks associated with devices are multifold in different sociocultural and political contexts. Understanding these factors is critical to determine the feasibility and risks associated with a tech-enabled education intervention. What types of education services is the organization providing? Who owns the device? Who is also sharing the use of the device (e.g. family members)?

What is the device used for? How often do they have access to wi-fi? For instance, in a refugee camp in Lebanon, one device is usually shared amongst several tents that is used by parents to contact their children on safety matters.[1] Their children may share another device while traveling in groups to school and crossing insecure areas. [2] The application of any Ed-tech in this environment would require a tremendous amount of care in its delivery and design of education contents in order to ensure privacy and security.

Examples of factors that could impose risks to children with the use of devices:

1. The details of **social and family structures** matter in the context of intervention. Lynda Kigera from Norwegian Refugee Council mentioned the challenge to persuade the fathers, who they found to be the phone owners within families, on the necessity of providing psychosocial support to children. Such a situation creates an instance where a child may be deprived of access to education services as it is not perceived by the technology owner as being important. Understanding children's relationship with families and the related sociocultural context is going to be key to an effective response.

2. **Unrestricted access** to digital devices can also pose risks to children. Parents may have no control over what information the children are exposed to. When children are connected online, they may be subjected to harm from news, social media, fraudulent messages, explicit contents, and other sensitive information related to ethnic, cultural, religious, or sexual identities. Displaced children are particularly vulnerable to these harms throughout their journey. This vulnerability is compounded with tendencies to make immature decisions, the lack of help from adults and safeguarding institutions, and the absence of easily applicable legal framework.

3. **Digital exclusion** is an inevitable byproduct of digital intervention. And it can be exasperated by gender. In some countries, boys are 1.5 times more likely than a girl to own a phone and 1.8 times more likely to own a smartphone.[3] In addition to the gendered digital divide, Lynda Kigera raised concerns over girls' responses to a lack of access to the internet for receiving digital education.

   Similarly, other vulnerable groups of children, such as the disabled or those who suffer from mental health problems, are all subjected to digital exclusion in one way or another. In displaced communities, these discrepancies are likely to be more salient than usual.

1 M. Alfarah and Bosco Paniagua, M. A. (2016). 'The Role of ICTS in Rebuilding Education in Areas of Armed Conflicts: The Syrian Case.' Paper presented at the International Conference on Education and New Learning Technologies, Barcelona, Spain. Retrieved from: https://doi.org/10.21125/edulearn.2016.0359

2 Ibid.

3 Digital Safeguarding for Migrating and Displaced Children. PDF. Save the Children, 2020.

> *Imagining that you're not able to continue your classes for the day because you cannot afford the data bundle, translated to finding negative coping mechanisms, especially for young girls such as 'I'm going to find a boyfriend who's going to buy me airtime or data bundle', I might feel like I owe them so 'I need to exchange something for that data bundle', so 'I might video chat them' and other crazy things, just because I need access to a data bundle for my classes.*"
>
> — **Lynda Kigera,** Global Roving EdTech Advisor, Norwegian Refugee Council

Response agencies can learn from plenty of existing cases involving the use of devices in Ed-tech in the humanitarian space. For instance, a pilot project from Save the Children for Syrian refugee and host community children in Jordan[4] realized not all children in target schools had access to phones. The project provided the schools with a library of smart phones to lend devices to students in the short term, so as to ensure a fair access to education resources. As a safeguarding method, the phones had pre-downloaded math contents and were locked from being used for other purposes or accessing open internet. All in all, devices must be introduced with deliberation that reflects an awareness of local contexts.

4 Displaced Children and Emerging Technologies. PDF. Save the Children, 2017.

Data

Ed-tech is widely used for short-term informal learning purposes and for long-term accreditation purposes. The extent to which information is collected is based on the nature of the intervention. Is it needed for a short-term purpose such as helping children transition to traditional education systems? Is it needed to fill a temporary education gap? Or is it being used to fulfill longer-term educational requirements? Generally, data abuse or leakage may mean infringement of privacy or fraud to ordinary people. But, for displaced groups, it could mean life or death.

> *"The data we collect has to do with your location of origin, which can easily be associated to your ethnicity or your religious affiliation and, in many contexts, that's actually a reason for persecution."*[5]
>
> — **Pietro Galli**, Director of Technology, Norwegian Refugee Council

Digital Safeguarding for Migrating and Displaced Children by Save the Children outlined the risks of collecting biometric data (including facial recognition data), location data, DNA data, anonymized and de-identified data, metadata, and group data. They stressed the need to review all these risks before for any intervention containing data-collection is conducted.[6] Generally speaking, there are three principles recommended to response agencies:

1. **Minimize the collection of personal data.**
2. **Leverage existing efforts in data collection.**
3. **Build common agreements and principles across agencies in the collection, use and storage of data.**

The three principles highlight the idea of building resilience against potential risks through minimizing the nodes in the data network. And, whenever technology is required, one way of strengthening the information exchange is with the use of secure technology. For example, the Protection-Related Information Management (Primero) application[7] was developed to make the handling of data easier for humanitarian workers at frontlines while emphasizing security and confidentiality for vulnerable children.[8] It helps partners to securely collect, store, manage, and

5 Berenice Healey. "Norwegian Refugee Council: The Importance of Tech Training for Displaced People." Verdict. October 02, 2019. Accessed December 29, 2021. https://www.verdict.co.uk/norwegian-refugee-council-technology/.

6 Displaced Children and Emerging Technologies: Save the Children's opportunities for investment and impact. PDF. Save the Children, 2019.

7 Displaced Children and Emerging Technologies. PDF. Save the Children, 2017.

8 Ibid.

share data in order to perform a wide range of tasks to apply or scale up digital intervention. [9] In such a space involving children, data protection needs robust technical innovation to mitigate potential risks.

Leveraging existing efforts in data-collection can serve at least three purposes:

1. Increasing the efficiency and effectiveness of data collection. In some cases, repetitive biometric registration amongst refugees and displaced communities has become a problem that leads to registration fatigue. [10] Not only did the trustworthiness of all agencies decrease among the beneficiaries in that example, but the accuracy of the information was somewhat unreliable due to low cooperativeness.
2. Addressing the potential sources of leakages from all stakeholders. These stakeholders involve everyone in the process from responders, to children, to parents, to the government to the school officials. Monitoring data security along the process of implementation can be challenging but tightening the weak nodes in the web of information security is essential for a risk-free digital intervention to displaced children's education. In terms of fostering multilateral cooperation in addressing the digital safety concerns, there needs more efforts to build common agreements and principles for intervention.
3. Sharing resources and technologies. The ability to share costs is beneficial for the non-for-profit sectors that bear higher risks in delivery of digitized humanitarian aid. Rakesh Bharania, director of humanitarian impact data at Salesforce.org, has mentioned that nonprofits tend to focus more on sustainability and supportability rather than investing in back-end issues as they have proven to be less appealing to donors.[11] It is not hard to imagine that the same concerns apply to Ed-tech enabled interventions. Therefore, a network of collaborating actors could support each other regarding the various risks and build capacity through partnerships or shared resources.

To expand on the complexity associated with children, there needs to be greater investment to bring clarity of data consent as well as data use and security. Ethical concerns within humanitarian interventions, where displaced or vulnerable populations are inevitably inclined to behave in a passive manner to receive aid, need to be considered. How can an organization make sure that data consent is free from implicit coercion? To what degree children need to be informed on the data consent might be dependent on various factors such as their age, or ways of participating. If complicated or the children are too young, one may need to communicate with their parents in order to receive valid consent. Beyond basic consent, there are special considerations that must be considered. For example, a displaced community may be more cautious to interact with organizations who are trying to help if such organizations are perceived to be supporting efforts by an unfriendly government. Agencies must be aware of their responsibility and consider with deliberation, who should be empowered to make decisions around the consent of children's data.

9 Ibid.

10 Displaced Children and Emerging Technologies: Save the Children's opportunities for investment and impact. PDF. Save the Children, 2019.

11 Catherine Cheney. "Delivering Digital Aid When the Internet Becomes a Weapon of War." Devex, January 28, 2022. https://www.devex.com/news/delivering-digital-aid-when-the-internet-becomes-a-weapon-of-war-102522.

Future Considerations

1. **Risk-benefits analysis needs to be conducted carefully in every context in an effort to mitigate risks and ensure fair access to education resources through the use of Ed-tech.** This process involves understanding why the children are displaced; what risks they face throughout their journey; what type of sociopolitical context and family structure exists in the region; what related government and multinational organization efforts already exist; and how effective other interventions have been. A full scope of relevant questions is contingent on the intervention purposes, environment, and target group.
2. **Localization or contextualization of the Ed-tech should be assessed by local stakeholders that understand the risks in the space.** Teachers and parents are great resources to provide insights into safeguarding children in their use of technology in the local context.
3. **In most cases, supervision by and of adults is necessary to ensure that children are guided throughout the learning experience.** The use of Ed-tech should not intervene with an intention to replace the role of teachers or parents. Yet, inattention to the potential harms from families or institutions that may act as source of gender-based violence and deprivation of rights to access education services, will be a drawback to all efforts for protecting displaced children.
4. **Addressing the tech security issue in tandem with other infrastructure challenges is crucial to safeguard displaced children as a whole.** Risk factors such as unstable internet connections, inaccessibility to basic resources and lacking a safe operating environment are obstacles and often beyond the capacity of agencies in the education space. A holistic effort in addressing the risks facing displaced children will aid a safe application of Ed-tech.
5. **Leveraging existing multilateral efforts to establish long-term agreements and principles on the use and storage of data.** A robust collaboration mindset across agencies is crucial to ensure the safety of children for any Ed-tech related intervention. Agreements must entail rules and regulations surrounding security and privacy standards; long-term considerations; and local partnerships.

Bibliography

Alfarah, M., and Bosco Paniagua, M. A. (2016). 'The Role of ICTS in Rebuilding Education in Areas of Armed Conflicts: The Syrian Case.' Paper presented at the International Conference on Education and New Learning Technologies, Barcelona, Spain. Retrieved from: https://doi.org/10.21125/edulearn.2016.0359

Cheney, Catherine. "Delivering Digital Aid When the Internet Becomes a Weapon of War." Devex, January 28, 2022. https://www.devex.com/news/delivering-digital-aid-when-the-internet-becomes-a-weapon-of-war-102522.

Digital Safeguarding for Migrating and Displaced Children. PDF. Save the Children, 2020.Cheney, Catherine. "Delivering Digital Aid When the Internet Becomes a Weapon of War." Devex, January 28, 2022. https://www.devex.com/news/delivering-digital-aid-when-the-internet-becomes-a-weapon-of-war-102522.

Displaced Children and Emerging Technologies: Save the Children's opportunities for investment and impact. PDF. Save the Children, 2019.Displaced Children and Emerging Technologies. PDF. Save the Children, 2017.

Healey, Berenice. "Norwegian Refugee Council: The Importance of Tech Training for Displaced People." Verdict. September 30, 2019. Accessed November 03, 2021. https://www.verdict.co.uk/norwegian-refugee-council-technology/.

Tebbe, Kerstin. Norwegian Refugee Council Education Responses in Urban Setting. Report. Norwegian Refugee Council, 2016. 1-34. Accessed November 3, 2021.


DH Network
Digital Humanitarian Network