Julio Cesar Aviles/Save the Children

DIGITAL SAFEGUARDING FOR MIGRATING AND DISPLACED CHILDREN

Save the Children

An overview of the current context and trends, potential risks and practical next steps

Save the Children's Migration and Displacement Initiative

Farjana Sultana / Save the Children

Acknowledgements

The author would like to thank Steve Morgan, Josiah Kaplan, Ilana Tyler-Rubinstein, and Madeleine Maxwell-Hart from Save the Children's Migration and Displacement Initiative for providing guidance and input throughout the research process. Additional gratitude goes to Save the Children Denmark for commissioning this report, and Danida/Danish MFA for funding this work. Additional thanks are in order for staff from Save the Children offices in Lebanon, Ethiopia, El Salvador, The Balkans, Afghanistan, the UK, Norway, Denmark, the US and Switzerland for sharing their experiences and knowledge of how digital programming intersects with child migration and displacement.

Appreciation is extended to external agencies including UNHCR, OCHA, UNICEF, The Engine Room, New York University's GovLab, Yale University, ChildFund, World Vision, and InterAction for sharing their insights, and to all those who have shared guidance and research on the use of digital technologies in programming with children who are migrating or displaced. A special thank you to the project's steering group members: Arij Boureslan, Menaca Calyaneratne, Albert Den Boogert, Susan Grant, Sofyen Khalfaoui, Alice Moltke Ladekarl, Hannah Newth and Dominiek Vangaever.

Researcher and lead author: Linda Raftree
Copy editing: Lisa Findley and Nicola Kiess
Graphic design: John McGill

MINISTRY OF FOREIGN AFFAIRS
OF DENMARK
Danida

Contents

Abbreviations and Acronyms

CDR	Call data records
COPPA	Children's Online Privacy and Protection Act
DNA	Deoxyribonucleic acid
EU	European Union
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GSMA	Global System for Mobile Communications
HHI	Harvard Humanitarian Initiative
HIF	Humanitarian Innovation Fund
HIV	Human immunodeficiency virus
ICE	Immigration and Customs Enforcement
ICRC	International Committee of the Red Cross
IFRC	International Federation of the Red Cross and Red Crescent Societies
ICT	Information and communications technology
ID	Identification document
IOM	International Organization for Migration
IT	Information technology
ITU	International Telecommunication Union
LGBTQI	Lesbian, gay, bisexual, transgender, queer/questioning and intersex
MDI	Migration and Displacement Initiative (of Save the Children)
M&E	Monitoring and evaluation
(I)NGO	(International) non-governmental organisation
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
PIM	Protection information management
RD4C	Responsible Data for Children
RIL	Response Innovation Lab
UAVs	Unmanned aerial vehicles
UK	United Kingdom
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNDG	United Nations Development Group
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations International Children's Emergency Fund
UNODC	United Nations Office on Drugs and Crime
US	United States
WFP	World Food Programme

Defining digital technology and innovation

In this report, we use the terms digital technology, innovation, tools and approaches to refer broadly to:

- the use of mobile devices such as phones or tablets;
- the collection and use of digital data;
- general positioning systems (GPS) and sensors;
- biometrics (e.g. digital fingerprints, iris scans, and facial recognition);
- big data and associated approaches (e.g. data analytics, artificial intelligence, machine learning, deep learning, sentiment analysis, and predictive analytics);
- social media platforms and associated content; and
- other tools, platforms, applications, or approaches that rely on mobile data, the internet, digital data, or advanced computational capacity to function.

FOREWORD

Marieke van der Velden / Save the Children

An estimated 34 million children and youth are forcibly displaced[1] and many more are on the move in search of economic and educational opportunities. Digital connectivity, digital data and emerging technologies are changing how displaced people inform themselves and access information and communicate, as well as how agencies conduct and manage their programming and measure impact.

Aid organisations increasingly rely on data, and emerging, new technologies to improve their reach and assist vulnerable, hard-to-reach populations, including children on the move. The ongoing COVID-19 pandemic accelerates the aid sector's desire to develop digital solutions to support vulnerable populations, including for migrant and displaced children. However, increased connectivity among these populations has the potential to increase risk. The rapid introduction of technological innovations poses new ethical dilemmas and threats to the safety and wellbeing of displaced children as national legislations struggle to keep pace.

Save the Children's Migration and Displacement Initiative (MDI) is itself an innovator; developing, inter alia, technology driven tools to enable a safer and more impactful response to support the most vulnerable children on the move. The Predictive Displacement tool is one such example – a prototype model for anticipating the future scale and duration of conflict-driven displacement crises. To compliment such work, the MDI has simultaneously commissioned the following report to support improvements in Save the Children's child safeguarding in situations where digital technologies 'interface' with migration and displacement contexts.

This Digital Child Safeguarding report follows recommendations from the MDI's and Save the Children Denmark's 'Child Displacement and Emerging Technologies' study[2] and addresses relevant recommendations raised in Save the Children's Global Audit in 2016. The learning from this report will support Save the Children's internal capacity-building regarding responsible applications of technology for M&D-relevant child and youth programming, and at the same time, provides a significant and timely contribution to emerging sector-wide digital child safeguarding good practice. We anticipate a secondary phase of this research in 2021 to support the development of guidance and decision support tools that equips the organisation and the sector with the necessary instruments for digital child safeguarding and the broader digital transformation agenda.

Data and technological innovation are not the 'enemy' – they offer great and much needed capacity for positive and transformative change in our sector. Nevertheless, as the scale and influence of technology increases, aid actors **must be** equipped with the proper digital safeguarding mechanisms to prevent harm to the very children they seek to keep safe, as well as to reduce any legal or reputational risks. Equally, the increasing reliance on digital technology should not neglect those without access. We increasingly see examples where we risk contributing to the 'digital divide', as big data and tech-based programming overlook those without connectivity. Identifying how we collectively and effectively navigate these myriad challenges, without jettisoning the opportunities offered by technological innovation, is a challenge the aid sector must confront rapidly. For that reason, I hope that this report will help frame the challenge for both practitioners and policy makers and encourage the immediate prioritisation of 'digital safeguarding'.

Steve Morgan
Director
Migration and Displacement Initiative
Save the Children International

CJ Clarke / Save the Children

Sierra Leone Country Office

EXECUTIVE SUMMARY

The potential for digital to transform programming

An estimated 34 million children around the world have been forcibly displaced from their home[3] – and this number is growing year on year. Digital technologies have the potential to transform programming with migrant and displaced children by making it easier to reach and assist mobile populations, increasing efficiencies and driving improvements in programme quality, enabling Save the Children and other agencies to deliver greater impact for some of the world's most vulnerable children.

Yet the rapid pace of digital change poses challenges for a sector with limited capacity and resources, as well as risks and threats to the safety and wellbeing of displaced children. Children who are vulnerable *offline* are also likely to be vulnerable *online*, particularly girls, LGBTQI youth, and migrant and displaced children. The COVID-19 pandemic has also highlighted the challenges of a wholly digital approach. Despite increased digital connectivity, some displaced populations still lack access to devices and many do not trust agencies to collect and use their data, which can lead to the exclusion – or self-exclusion – of children who would benefit most from digital programmes.

If the sector is to successfully harness the enormously positive and transformational potential of emerging technology, then it is vital that we develop and embed digital safeguarding guidance and policies that are agile and flexible enough to keep up with the rapidly changing digital landscape.

If we want to harness the positive benefits of digital technologies while protecting the displaced children that we serve from potential harm, Save the Children and other agencies urgently need to build greater digital capacity, knowledge and skills, so that we can fully assess the child safeguarding risks of emerging technologies and implement policies and practices to mitigate them. These must be agile and flexible enough to keep up with the pace of change in areas that do not yet have clear legal frameworks.

In this study, we build on our 2019 report 'Displaced Children and Emerging Technologies' and set out how the sector is responding to child safeguarding risks posed by digital technology, and our recommendations for immediate and practical next steps to ensure that every migrant or displaced child can benefit from digital innovation and stay safe.

Our research involved interviews with Save the Children employees across the US, the UK, Kenya, Denmark, Switzerland, Lebanon, Ethiopia, El Salvador, Afghanistan and the Balkans as well as external technology and innovation experts within the aid sector. These interviews were supplemented by a comprehensive literature review of academic, organisation and sector reports and documents. Learning from this research will support Save the Children's internal capacity building and provide useful recommendations for the sector as a whole, helping us to ensure that digital technology is used responsibly and where appropriate in programming aimed at migrating and displaced children and young people.

Safeguarding risks introduced by digital programmes

There are four main areas of child safeguarding risk in the context of digital migration and displacement programmes.

1

Exclusion and self-exclusion

Children without access to devices are excluded from digital programming and digital datasets, so they may be unable to access some services and agencies may be unable to plan and deliver programmes effectively due to missing children's data. Self-exclusion occurs when children opt out of digital programmes, often because they lack trust in how their data will be used or have privacy concerns.

2

Harm caused by humanitarian innovation

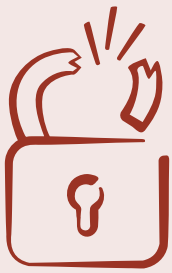
Innovation carries inherent risk, especially when using untested technology with vulnerable populations (e.g. product development and testing of mobile money platforms or contact tracing apps). Aid agencies may not have the same expertise in digital technology as the companies that provide the technology, so could be at a disadvantage when assessing the potential risks or harm that innovation might bring to migrating or displaced children.

3

Increased exposure to online harms

Agencies can inadvertently expose children to risks when they provide them with devices or access to the internet, encourage them to use the internet or social media, engage with them via social media, or use children's images or stories online. Social media can amplify existing risks for migrating and displaced children, who can be more vulnerable to online abuse, bullying or exploitation.

4



Data misuse or mishandling

Agencies collect highly sensitive information including biometric data, DNA and location data in order to serve and protect children, but they may be unaware that this data can be misused even when encrypted, non-personalised or anonymised. When working with multiple partners, donors, governments and private sector organisations, there can be a lack of clarity about how to manage data sharing and who has responsibility. Furthermore, it can be hard to determine the extent to which children's data is protected and by which regulations when agencies are serving people from and across multiple countries.

Underpinning these risks are a number of cross-cutting issues that profoundly impact our collective capacity to identify, prevent and mitigate child safeguarding risks. These include:

- **Digital literacy:** many humanitarian actors have a limited understanding of how digital data and data analytics influence migration and displacement programmes.
- **Capacity challenges:** these exist for all agencies, including the largest and most well-resourced, but the challenge is greater for smaller agencies and 'local' child safeguarding partners, who can struggle to meet aid agencies' or donors' strict social media policies because they lack the knowledge, capacity, systems and budgets to do so. Local partners often do not have the capacity to implement the necessary systems to manage data securely or do not report child safeguarding incidents because they do not have an appropriate system in place. Failure to implement appropriate digital safeguarding policies can also be a result of poor (or no) translation into local working languages. This is a particular concern for the global drive for greater localisation.
- **Trust:** refugees and migrants do not always trust agencies to properly collect and protect their data, sometimes rightly so. Stories of data being misused by policing authorities are prevalent, particularly for the purpose of tracking and tracing individuals. Lack of trust in agencies to use data ethically can result in children opting to exclude themselves from digital programmes, often those who would benefit most from such interventions.

Current digital safeguarding policies and practices

Save the Children has a strong base of child safeguarding and data security policies upon which to build a more robust digital safeguarding effort. There are high levels of awareness and critical thinking regarding the impact that digital devices and new and emerging technologies have on children. The organisation recognises the opportunities that digital technology and innovation provide in the battle to prevent the harm or exclusion of children.

Across the sector, most existing safeguarding policies and practices do not consider the risks associated with changes in the emerging digital environment.

Staff awareness of safeguarding issues within digital programming is also high in many areas, including awareness of the digital divide and how lack of access can lead to exclusion of vulnerable children; how online bullying might lead to self-exclusion; the benefits and potential risks that arise when children use the internet and when Save the Children uses digital platforms in its work; and data security and privacy.

Across the sector, most existing safeguarding policies and practices do not consider the risks associated with changes in the emerging digital environment. The lack of an ethical and child safeguarding specific framework could expose children as well as agencies and partners to unnecessary risk. Until now, discourse with aid agencies and donors has largely focused on *protecting* children online (e.g. from trafficking and exploitation). Very few existing resources address the specific intersection between child safeguarding and digital programming or innovations.

Recommendations for improving digital safeguarding in the aid sector

If the sector is to successfully harness the enormously positive and transformational potential of emerging technology, then it is vital that we develop and embed digital safeguarding guidance and policies that are agile and flexible enough to keep up with the rapidly changing digital landscape, adaptable to the different contexts we work in, and regularly updated. Investment in our collective capacity to benefit from digital technology and respond to its challenges must be prioritised if we want to deliver greater impact for migrant and displaced children and keep them safe.

This report identifies seven key aims that the sector should focus on to prevent the harm or exclusion of children in digitally led programmes.

1 

Ensure digital inclusion for all

Programmes should seek to improve digital access for children because of the significant benefits this can bring, but programmes must be inclusive for children without digital access to avoid excluding certain target populations. Expanding datasets to incorporate individuals both with and without digital access will avoid skewed insights.

2 

Establish trust in the system

Lack of trust is a key barrier to children participating in digital programming, so ensuring that children's data is not misused by authorities, governments and the private sector is crucial in order to build their trust.

Further research on the extent to which a lack of trust in the system, agency or sector makes children reluctant to provide data may be useful. Exploration of additional barriers to data sharing among children would also be valuable to understand potential obstacles to participation in digital programmes and ways in which these could be overcome.

3 

Design clear innovation partnership frameworks

Partnering with private sector innovation companies brings many advantages and opportunities. However, there are also risks as they may have differing priorities or agendas. There is a need for clear policies, frameworks, due diligence checks, and risk-benefit assessments tailored to humanitarian innovation and public-private partnerships.

Risk assessments could draw on the Response Innovation Lab's innovation toolkit or Principles for Digital Development programming guidance. Core humanitarian principles could serve as a basis for assessing risks of implementing digital programming:

1. do no harm,
2. humanity,
3. neutrality,
4. impartiality and
5. independence.

These would need to be reoriented towards practitioners and adapted to the needs of migrating or displaced children.

4 Ensure that digital programmes reflect beneficiary needs and concerns

Participation and feedback from children and adults in local communities must be reflected in safeguarding policies, programming and advocacy work. Communities should be involved in the design and assessment of new digital programmes and their participation should be supported by the establishment of an ethical review board and clear channels for raising concerns and sharing results in a transparent manner.

5 Increase digital literacy and capacity in the sector

Agencies have a duty of care to safeguard children when they enable them to access mobile devices, the internet or other digital technologies but the capacity of staff working in the field and in local agencies remains a risk to effective digital safeguarding.

Local offices must have sufficient capacity to uphold child safeguarding that is contextually relevant and adaptable to keep up with emerging platforms and technologies. Streamlined guidance should be created and contextualised for the needs, resource levels and capacities of local organisations.

Support must be provided to local offices to help them adapt policies to fit local data protection regimes, establish point persons to provide specific guidance in local contexts, and align data storage and security systems so that offices don't have to manage multiple systems.

Training must be made available across organisations and partners to build awareness of the importance that data protection and digital safeguarding are "everyone's responsibility", as with traditional safeguarding.

6 Develop clear ownership, governance and training

Digital innovation moves more quickly than national legislation, so agencies need to develop policies and practices that are agile and flexible enough to keep up with the pace of change in areas that do not yet have clear legislation. In some cases, partner agencies present a risk because their less robust systems are unable to provide adequate data security.

Organisations must develop governance procedures that clearly stipulate who is responsible for which aspects of digital safeguarding policy and practice, and be clear about the level of skill and awareness needed to comply with policy. Responsibility should not be reliant on one staff member to manage, maintain and update procedures or systems.

Training must be made available across organisations and partners to build awareness of the importance that data protection and digital safeguarding are "everyone's responsibility", as with traditional safeguarding. Training should include how to address risks with metadata, the potential for re-identification of anonymised data, and other emerging issues with data and data privacy.

7 Develop practical and consistent data management systems and processes

The sector needs practical data protection and management guidelines that are contextually and operationally relevant. Agencies need also to invest in better alignment of systems for data storage and security.

Furthermore, agencies need to understand the reputational, legal and financial consequences of poor and inconsistent processes, as well as the sometimes significant consequences for the child. Ethical and legal counsel should be sought for any digital programming.

Further research is required, including additional regional and country level cases studies to ensure that any guidance and toolkits that are developed are practical and adaptable to local contexts.

Practical next steps

Current sector guidance on digital safeguarding is diffuse and complex. There are only a few resources addressing the specific intersection between child safeguarding and digital programming or innovations.

Collaboration with other agencies is crucial to build sector-wide norms, capacity and training resources for staff and management on digital child safeguarding.

These are actions that Save the Children and the wider sector can take now, not just for migrant and displaced children, but also to prevent online harms to children more widely.

Develop a toolkit for digital safeguarding that includes:

- **A** Safeguarding guidance and policies for new digital innovation programmes, which can be adapted to local contexts and supported by training.
- **B** A risk assessment tool that can be used when working with private sector partners or local agencies. Risk assessments must include specific questions about innovative approaches, data protection and security (e.g. risk of data monetisation), digital technology, data sharing, and emerging safeguarding risks.
- **C** Clear communication channels for staff, partners and beneficiaries to voice concerns.

Review and update safeguarding, social media, data protection, data security and informed consent policies so that they are contextually specific, adapted to the local language and regulations, and consider new technologies and most frequently used digital platforms (e.g. WhatsApp and Facebook groups).

Develop research, monitoring, and evaluation frameworks to identify and address short- and long-term benefits, risks and harms from experimentation and innovation.

Develop a regulatory framework with partners to ensure sufficient capacity and technological understanding.

Work with private partners to stay up to date with which devices and online platforms children are using, how they are using them (e.g. borrowed devices, restricted use) and their attitudes towards them (e.g. affordability, purpose of use, privacy concerns, experiences of harm).

Invest in training with regional and country offices to improve the digital literacy of their staff and emphasise the associated child safeguarding risks and how to mitigate them.

Establish focal points within the organisation to establish best practice and provide guidance on data privacy and protection in national contexts.

Invest in better alignment of systems for data storage and security so that country offices are not managing multiple systems, depending on member office resources and preferences.

Lucia Zoro / Save the Children

Key components when developing a digital intervention

- **Embed clear agreements and assessments** about which data can be **shared with government and private sector** and for what purposes.
- Consider building in **mixed mode data collection** (e.g. offline and online) when designing programmes so that they are not skewed towards children with access to technology.
- **Build community participation** early in the implementation phase to address concerns at a local level.
- Establish an **internal ethics review board** during programme planning and implementation.
- Undertake a thorough **risk assessment** that considers data management and security, data sharing and use, digital technology and innovation, and emerging safeguarding risks.
- **Provide training** to ensure staff have the appropriate skills to **carry out risk assessments**.
- **Seek legal counsel** to establish necessary agreements with innovation and/or digital partners.

This report identifies some further core good practices for practitioners in addition to these practical next steps, which will help to ensure that every migrant and displaced child can reap the benefits of digital programming and stay safe.

Francesco Alesi / Save the Children

INTRODUCTION

The adoption of new technology in the sector seeks to improve efficiencies, enhance decision-making capabilities and drive improvements in programme quality. Yet, the prevalence and pace of technological innovation highlights an urgent need for a programme of comprehensive and robust support to ensure that the use of new technologies does not cause unintended harm to children.

Save the Children is a recognised sector leader in child safeguarding. This report recommends the next steps the sector should take to ensure strong digital child safeguarding policies and practices are implemented, so that we can harness the benefits of digital innovation, mitigate the risks and navigate any safeguarding issues that arise.

In 2019, a Save the Children study on emerging digital technologies in programming with migrating and displaced children identified a number of gaps in terms of harm mitigation and recommended that Save the Children strengthen its organisational digital safeguarding practices.[4] This report was commissioned to inform the development of practical frameworks and tools that Save the Children and other agencies can use to help mitigate risks arising from the adoption and use of emerging digital technologies in child migration and displacement programming and advocacy.

Aid agencies are incorporating current and emerging digital tools and technologies into various aspects of their programming and operations. The arrival of the COVID-19 pandemic in early 2020 and subsequent government-mandated restrictions on group assembly –– have forced the sector to quickly become more dependent on new and emerging digital technology to reach and support vulnerable populations. Organisations are working to identify ways to implement their programmes remotely or online, where possible.

Digital technologies and innovations have enormous potential to transform programming with migrating and displaced populations, in particular to support case management and family reunification.[5] Nevertheless, digital technologies introduce ethical dilemmas, risks and potential harm especially for those children who are already vulnerable.

Safeguarding and child protection policies and practices have not kept pace with technological change. Most organisations operate within traditional safeguarding policy and practices that do not consider the risks associated with changes that are happening in the emerging digital environment. This leaves the most vulnerable children open to safeguarding risks that must be mitigated if we are to protect the children we serve from potential harm.

Despite the general lag in digital safeguarding policy and practice across the sector, pockets of good practice were developing before the COVID-19 pandemic. There is an opportunity for Save the Children to adapt and strengthen existing protocols and procedures and set in place good practices for digital child safeguarding that will benefit and protect children now and in the future.

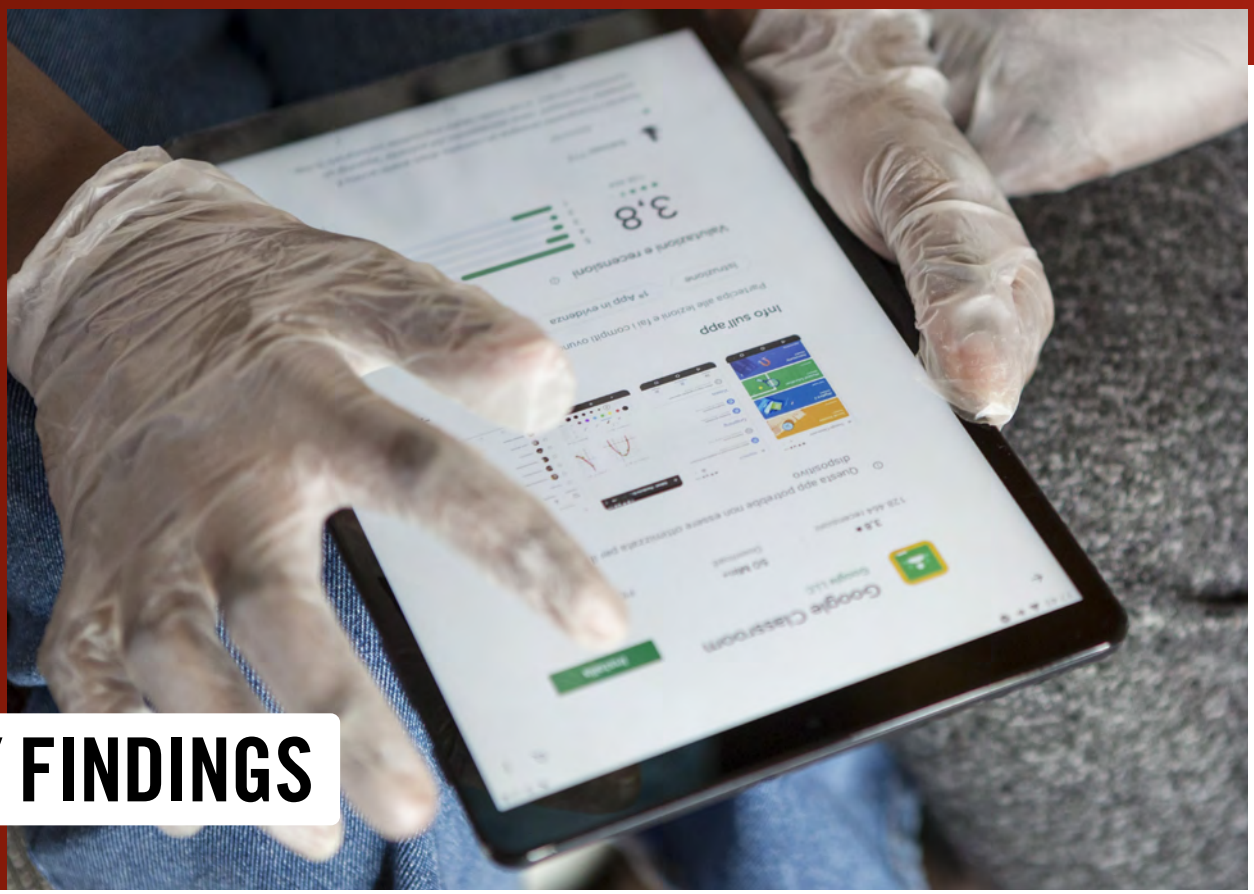
Safeguarding and child protection policies and practices have not kept pace with technological change. Most organisations operate within traditional safeguarding policy and practices that do not consider the risks associated with changes that are happening in the emerging digital environment.

Fieldwork for this report took place from December 2019 until April 2020. Key informant interviews were conducted with 47 Save the Children staff across the US, UK, Kenya, Denmark, Switzerland, Lebanon, Ethiopia, El Salvador, Afghanistan and the Balkans and 12 other agencies (see Annex 3 for details). They covered both pre-COVID-19 safeguarding and programming approaches as well as the shift from 'normal' programming to digital and remote programming as a result of the COVID-19 pandemic.

This report:

- explores existing digital safeguarding policies and practices for migrating and displaced children;
- assesses the risks of digital programming and Save the Children's management of digital safeguarding;
- identifies a risk framework for Save the Children to use for digital safeguarding in programming; and
- recommends next steps for Save the Children and the wider sector to ensure that we can harness the benefits of digital programming while protecting children from harm.

It should be emphasised that this report is not a formal evaluation, nor does it attempt to offer a final set of guidance, tools or templates. Rather it draws from the experience of the sector and existing literature to highlight gaps in digital child safeguarding and provides recommendations for Save the Children and other aid agencies to improve digital safeguarding across their operations. We hope it facilitates discussion among Save the Children and other agencies about the guidance and support that is needed for more systematic implementation of digital safeguarding throughout the programme cycle.



Francesco Alesi / Save the Children

KEY FINDINGS

Digital technology is omnipresent in the year 2020[6] and has the potential to bring enormous benefits for programming with migrating and displaced populations. New data analytics approaches can be used to forecast mass displacement and support digital case management systems, dramatically improving aid agencies' capacity to respond to and support a child's migration journey. The COVID-19 pandemic has demonstrated that access to basic technology and social media channels is critical to enable agencies to deliver their programmes, communicate with affected communities, disseminate public health and virus-prevention information, and carry out needs assessments.[7]

Nevertheless, the increased use of digital technology and innovation creates ethical dilemmas for aid agencies. New technologies bring new, complex and constantly changing risks to children's safety. Until now, discourse within child rights agencies and donors has been largely focused on protecting children online from external threats such as grooming, pornography, child trafficking, exploitation and bullying. The sector is only now starting to explore how to address newly emerging risks, and considering the ways that they may inadvertently introduce or increase risks to children and communities as they expand their own use of digital technologies and data capture.

Digital technology can be a valuable tool for improving the efficiency, breadth and depth of services that aid agencies can deliver, and digital data can improve targeting of services and tracking of benefits. However, some agencies are worried that efficiency and innovation are currently being prioritised over efficacy and quality.[8] Donors have sometimes spurred the use of advanced technologies and the collection of large quantities of personal data because they see these as enablers of improved cost-efficiency and fraud prevention. Agencies, on the other hand, may view beneficiary data as an asset for understanding programme contexts and improving delivery.[9]

As data has grown in value, it has become a valuable commodity to offer when seeking funding. Aid agencies should weigh the potential gains of this approach against the potential negative impacts for affected children and communities. Holding large quantities of personal or sensitive data opens agencies up to legal and reputational risks related to misuse or poor management of data. A data leak because of weak compliance with IT security protocols or a breach due to a hacking or phishing incident could lead to a serious public scandal or legal action, as well as significant risks of harm for the data subject or subjects. Data accessed in such an incident could allow malevolent actors to harm, misinform, or undermine trust in a single institution or the humanitarian sector as a whole.[10]

Aid organisations must constantly ramp up their understanding of data protection issues and update their internal policies to keep pace with the rate of technology development and rapidly changing data privacy laws around the world.

To date, most agencies' approaches to digital safeguarding has focused on protecting children from harm while using the internet. The increased emphasis on data protection and privacy globally has encouraged the sector to also focus on the digital and data-related risks that its own programmes may introduce. Aid organisations must constantly ramp up their understanding of data protection issues and update their internal policies to keep pace with the rate of technology development and rapidly changing data privacy laws around the world. Save the Children, for example, rolled out an updated global data protection policy in 2017 to align with the European Union's General Data Protection Regulation (GDPR), which came into force in May 2018. Furthermore, both COVID-19 and the Grand Bargain[11] are pushing agencies to localise their approach. Agencies must not only shore up their own digital safeguarding skills and capacities, but they must also find ways to support local partners to do so.

The remainder of this report outlines the risks associated with digital technologies, reviews how Save the Children and the wider sector are currently managing these risks through policy and practice, and proposes recommendations to improve risk mitigation in areas where gaps are found.

Typology of digital risks for migrating and displaced children

This study identified four categories of risk as a result of the adoption of digital tools and programmes.

1. Exclusion and self-exclusion
2. Harm caused by humanitarian innovation
3. Increased exposure to online harms
4. Data misuse or mishandling

These areas are intimately interconnected. Risk factors comprise access to digital tools and connectivity; knowledge and capacity about new technology and digital data; overlapping roles and interests (primarily of children, families and communities, the aid sector, the private sector, governments, and non-state actors); ethics and power dynamics; transparency and accountability; and trust in the data gatherer.

Both individual agencies and the sector as a whole are unprepared to address this complex mix of technologies and risk factors. Agencies require greater capacity, knowledge, and skills to fully assess risks and harms and to implement policies and practices to mitigate them.

Figure 1
Typology of digital risks for migrating and displaced children

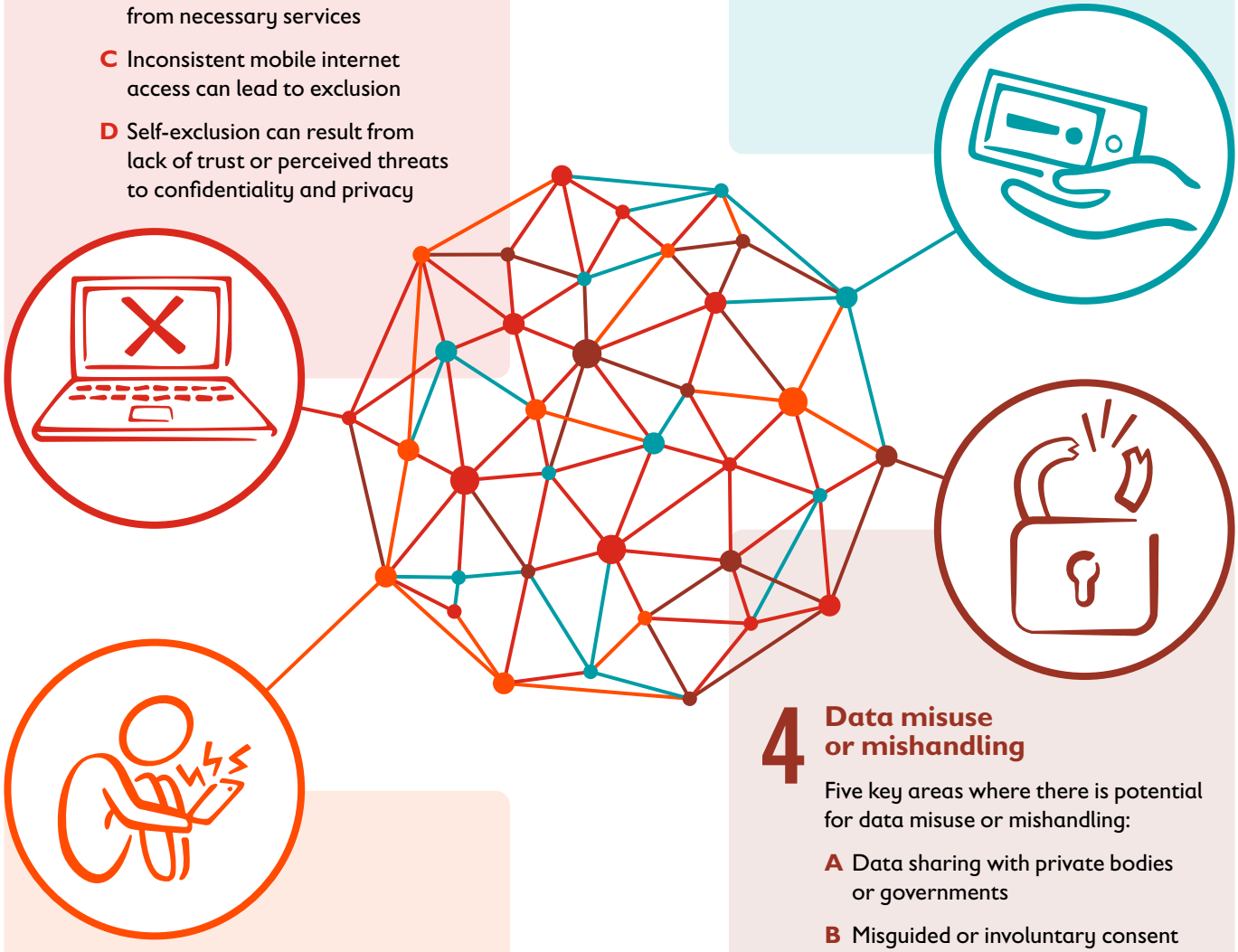
1 Exclusion and self-exclusion

The following exclusion risks can be generated by the introduction of digital technologies:

- **A** Lack of access to devices and the internet leaves certain children behind
- **B** Technology that is not tailored to children can exclude them from necessary services
- **C** Inconsistent mobile internet access can lead to exclusion
- **D** Self-exclusion can result from lack of trust or perceived threats to confidentiality and privacy

2 Harm caused by humanitarian innovation

- **A** Lack of accountability of the agency
- **B** Private sector priorities can undermine the needs of affected populations
- **C** Untested approaches add potential risk for vulnerable groups



3 Increased exposure to online harms

- **A** Agencies can unwittingly increase children's exposure to online harm through lack of guidance
- **B** Social media amplifies traditional risks for children in mixed migration or displacement contexts

4 Data misuse or mishandling

Five key areas where there is potential for data misuse or mishandling:

- **A** Data sharing with private bodies or governments
- **B** Misguided or involuntary consent
- **C** Enforced trade-offs between sharing data and receiving vital support
- **D** Varied legal frameworks across countries complicates multi-country programming
- **E** Lack of child focused data privacy laws in host countries

1 Exclusion and self-exclusion

Exclusion and self-exclusion refer to the risks of children and other beneficiaries being left out of digital programming and digital datasets. UNICEF warns that a 'digital divide' separates people who are digitally connected from those who are not, affecting how children communicate and access information. Factors that influence a child's online experience include the type of device they have access to, the level of their digital skills and education, their family income and the availability of content in their own language. Some children find themselves in a digital space where their language, culture and concerns are absent, which makes for an alienating or foreign online experience and leads to lower engagement and usage.[12]

The following exclusion risks are generated by the introduction of digital technologies:

A Lack of access to devices and the internet leaves certain children behind

Access to and use of digital devices, tools, platforms, and services have become more widespread globally over the past decade. By 2017, internet access through mobile data or fixed broadband was estimated to be available to more than 50% of the world's population.[13] Access tends, however, to be higher among wealthier, urban, male populations.

Agency adoption of digital technology has been moving at a rapid pace, yet many beneficiaries that agencies seek to serve have limited or no access to mobile devices or the internet and so are not able to benefit from online services. UNICEF estimates that nearly 9 out of 10 young people (aged 15–24) not currently using the internet live in Africa, Asia or the Pacific. Africa has the highest proportion of non-internet users among 15- to 24-year-olds. In Bangladesh and Zimbabwe, fewer than 1 in 20 children under 15 use the internet. Even if they do have access to a device, children may not use the internet due to poor connectivity and high data costs.[14]

Children may lack trust in digital platforms and therefore self-exclude. A child's identity and past experiences online may also affect participation.

When the COVID-19 pandemic erupted in 2020, the problem of digital exclusion was exacerbated as more agency services and programmes quickly moved online. Many people without access to mobile devices and the internet were left out; (staff reported that in some refugee and IDP camps, there was no access to even basic technology such as radios and televisions let alone smart phones, laptops and tablets). As this digital trend continues and perhaps increases, so too will the risk of exclusion. On the one hand, this may afford children and young people greater privacy. On the other lack of digital access means that some children do not have a 'digital footprint'. They are not represented in data and are thus unaccounted for when agencies generate insights, plan for and provide services, or make resource allocation decisions. Additionally, children without the ability to provide specific data (e.g. a digital ID) might not be able to gain access to digital programmes and services.

The United Nations High Commissioner for Refugees (UNHCR) notes that displaced populations face serious challenges in terms of connectivity across urban, camp and rural settings. There are still major gaps in data relating to digital penetration and ICT use and behaviours among displaced populations.[15]

B Technology that is not tailored to children can exclude them from necessary services

Biometrics, for example, have been designed for adults and may not work as well when used with children. For instance, facial recognition can be up to 3–5 years mistaken when assessing a person's age[16] and there are well-known challenges when it comes to identifying people with darker skin. Additionally, it is not yet clear if fingerprinting new-borns is effective. These kinds of errors in biometric recognition can lead to exclusion from vital services and barriers for marginalised and vulnerable groups including children.[17]

C Inconsistent mobile internet access can lead to exclusion

Many households share a phone, yet access might be unequal within the household. A global study by Girl Effect and Vodafone in 2019 surveyed 3,000 girls[18] and found that mobile access is often imbalanced, inconsistent, and strongly influenced by local gender norms. Rather than a binary distinction between 'no access to mobile' and 'access to mobile', girls highlighted that their mobile access is often changing and unreliable.

Gender and age are factors in phone ownership (not to be confused with phone access and use). Boys in some countries were 1.5 times more likely than girls to own any type of phone and 1.8 times more likely to own a smartphone. Young people aged 18 to 19 years-old more frequently owned phones than 15- to 17-year-olds.[19]

Some children who are disabled might have little or no access to a mobile phone, making them invisible in the digital world and in digital data. A 2019 study by the GSMA[20] found that disabled refugees in the Bidi Bidi camp were 68% less likely to have access to, own or use a mobile phone.

Caroline Trutmann Marconi / Save the Children

D Self-exclusion can result from lack of trust or perceived threats to confidentiality and privacy

Children often borrow or share phones, for example from a parent, an employer, an aid agency, or in the case of many girls, an elder brother.[21] This **makes access to sensitive information risky and reduces confidentiality**, so it may reduce the type of information that children, and girls in particular, seek or share online and encourage children to self-exclude. For example, where there are instances of domestic abuse or hazardous labour, children may want to explore options for migration or escape, but this becomes difficult when phone communication is controlled or accessible by others. Surveys that estimate mobile phone penetration by the number of households that own a device rather than by the number of children with their own device often miss this nuance.

Additionally, and especially in the case of girls, unrestricted versus restricted access to a device matters. Even when girls own devices, their use of those devices is often controlled or surveyed by family members, so for self-protection reasons girls may not be as free in their expression and exploration of information when using such devices.[22,23]

In the case of girls, unrestricted versus restricted access to a device matters… for self-protection reasons girls may not be as free in their expression and exploration of information when using such devices.

Children may lack trust in digital platforms and therefore self-exclude. Refugee and migrating populations may choose not to use apps and digital services if they do not trust the agencies who are promoting them or if they sense that using these apps or providing their data could put them at risk.[24] This can lead to self-exclusion, spurred by the need to protect oneself from invasive data practices and data sharing, or because apps could put them at risk.

Children might purposefully self-exclude by refusing to provide their data, providing false data, or simply not participating in programmes. Agencies should assess whether a lack of trust in the system, agency or sector makes children reluctant to provide data for fear that it can put them at risk.

A child's identity and past experiences online may also affect participation. Children who have been victims of bullying or other online abuse due to their identity may choose to self-exclude on online platforms or reduce their participation. Wider government policies and the extent to which there is freedom of speech also impact participation levels. In a 2019 qualitative research study in Jakarta, Indonesia, girls said that they commented less on social media platforms when the government increased online censorship of certain topics including reproductive health and sexuality, LGBTQI issues, political opinions, and blasphemy. Girls frequently mentioned high-profile media stories about individuals being beaten or arrested for online comments and explained that they had consequently stopped posting comments to avoid social media harassment.[25]

2 Harm caused by humanitarian innovation

Agencies are increasingly using emerging digital technologies to support migrating and displaced children, for example, technologies that help children access information, establish an identity (e.g. digital ID), or identify where to get support. Much of this innovation happens via public-private partnerships and may be driven by donor emphasis on innovation, scale, efficiency or accountability, or private sector interest in product development and testing, in addition to a drive to improve the experiences of affected populations.[26,27] Often aid agencies do not have the same expertise in digital technology as the companies that provide the technology. This means that they could be at a disadvantage when assessing potential risks or harms that innovation might bring to migrating or displaced children.

A Lack of accountability of the agency

Innovation carries some inherent risk of failure or mistakes because it involves experimentation. Humanitarian innovation with highly vulnerable groups such as children or crisis-affected communities raises the same kind of ethical questions as testing medical procedures and pharmaceuticals on extremely vulnerable groups. There are currently no mandatory or widely used frameworks in the development and humanitarian fields to guide and hold those conducting this kind of experimentation accountable.[28] Extra precautions are necessary when experimenting in a real-life setting and not in the safe confines of a lab.

Crisis affected populations such as refugees and displaced populations often have little choice about whether to participate in such experimentation, and many data privacy and ethics experts working in the humanitarian space believe that truly informed consent is not possible in crisis and emergency settings.[29] Innovation, if not conducted with a clear ethics lens and accompanying risk assessments, transparency, consent, duty of care principles and accountability to participating individuals and communities, has the potential to cause harm.

Critically engaging with the ethics and logistics of trialling new technologies with vulnerable populations will help protect those populations and hopefully contribute to better technology that will improve their lives.

B Private sector priorities can undermine the needs of affected populations

Partnering with governments and the private sector can enable scale and sustainability when operating in a particular country or context. The private sector brings much needed technical expertise and funding that can improve capacity and programming. Yet if not closely vetted and assessed, partnerships can lead to more harm than benefit. The private sector has more sophisticated technology expertise than aid agencies and it may have different priorities, which makes effective digital safeguarding and oversight difficult. This is complicated by agency fund deficits, which can tempt the sector towards partnerships that are less ideal or not fully vetted or evaluated.

Aid agencies, governments and the private sector all have an interest in deploying technology efficiently and cost-effectively, but efficiency, scale, and technology should not overshadow the experiences of affected populations. This impacts how funding is allocated, who leads innovation processes, and who primarily benefits from them.[30]

C Untested approaches add potential risk for vulnerable groups

There is currently a lack of data-related, legal regulation or protections in place for technological innovation in humanitarian contexts. The absence of clear policies, frameworks, due diligence checks, and risk-benefits assessments that are tailored to humanitarian innovation and public-private partnerships leaves vulnerable populations open to risk and potentially to harm. This is especially concerning when humanitarian innovations involve children from highly vulnerable or underrepresented groups. Untested approaches in uncertain environments carry a high risk and underscore the need for agencies to create a structured process for assessing risks and their effect on the most vulnerable.[31,32]

3 Increased exposure to online harms

Unintentional harm may be caused as a result of poor capacity to manage data in difficult contextual circumstances, but there is also the potential for harm to be present when adopting emerging approaches.

Agencies have a duty of care for safeguarding children when enabling them to access mobile devices and the internet or other digital technology. They can inadvertently expose children to online risks when they provide children with devices or internet connections, encourage them to use the internet or social media, engage with them via social media, or use children's images and stories online. Although many children and youth are already active online, when agencies enable internet or mobile access so that children can go online or post content by or about children, highly vulnerable children can be exposed to online risks without sufficient preparation. This might enable them to make risky choices or to access unsafe content. It might also expose them to persons and groups who wish to exploit or otherwise do them harm.

Multiple reports highlight situations where traditional risks including harassment and corruption, trafficking, gender-based violence, exploitation by policing authorities and recruitment by armed forces, have been exacerbated on social media.

As far back as 2013, a report by Plan International and the Oak Foundation noted that migrating children were using mobile phones and the internet to facilitate their migration or displacement experiences, allowing them to better plan their journey, locate safe points along the way, and check-in regularly with family and friends or safe spaces in their countries of origin, transit countries, and upon arrival.[33]

The following risks can arise by exposing children to the digital environment and social media:

A Agencies can unwittingly increase children's exposure to online harm through lack of guidance

Unguided digital access and a lack of awareness put children at risk.[34] Much has been written about online or 'cyber' risks for children and young people, which include cyberbullying, grooming, sexual exploitation, gaming addictions, changing norms and beliefs, recruitment into violent or extremist groups, self-harm, extortion, 'sexting', increased peer pressure, and loss of self-esteem from comparison with peers, which has been linked with an increase in depression and anxiety among adolescents and youth.[35–37]

In general, children who are at risk of abuse offline are also at risk online.[38–40] Evidence shows that those at greatest risk include: *"girls, children from poor households, children in communities with a limited understanding of different forms of sexual abuse and exploitation of children, children who are out of school, children with disabilities, children who suffer depression or mental health problems and children from marginalized groups."*[41]

Girls face greater risk of harassment online than boys, and the risk of cyberbullying is especially high for LGBTQI children.[42–44] Violence and discrimination, both on and offline, in their home countries may push LGBTQI youth to migrate, and they often become victims of violence and abuse during migration, if they end up in detention, and upon trying to integrate into countries of arrival. This is especially the case with transgender youth.[45]

Migrant children are at a higher risk of bullying than native children, as a study conducted in Italy reported[46] and the UNHCR warns that children on the move and those living in camps are at heightened risk of violence and abuse.[47] By extension, it can be assumed that refugee, migrating and displaced children are especially vulnerable to online abuse, bullying and exploitation.

B Social media amplifies traditional risks for children in mixed migration or displacement contexts

The risk of exposure to social media is an emerging area of research and children's experiences are still being explored as an increasing number of them go online. Multiple reports highlight situations where traditional risks including harassment and corruption, trafficking, gender-based violence, exploitation by policing authorities and recruitment by armed forces, have been exacerbated on social media. Examples of each situation are given below.

Harassment, corruption, violence and abuse by police, border officials, armed forces, civil groups, members of general public, and others

- Social media has been helpful for denouncing abuse of authority in El Salvador, yet the risk of retaliation is high and the lack of follow up by authorities makes individuals fear for their personal safety if they report abuse and are not able to do so anonymously.[50]
- In the Balkans, anti-migrant hate groups have been allowed to remain on Facebook, despite requests by other Facebook users to remove them.[49]
- Observers in Myanmar say Facebook pages were used to distribute hate and provoke violence against the Rohingya for months, if not years, before Facebook finally took action against them.[48]

Trafficking, deception and exploitation by smugglers

- Mobiles have made it easier for smugglers to exploit families through ransom demands for releasing their children[51] and social media can contribute to disinformation and misinformation that can put migrants at greater risk.[52] Smugglers publicise their services to reach people who have decided to migrate, and to entice those who have not necessarily been considering it. Some smugglers use social media to pose as NGOs tasked with organising safe passage to Europe by sea, or 'legal advisors' for asylum.[53–55]
- Traffickers can find a vulnerable child on an open channel and groom them to move to a 'dark channel' (a closed network), where traffickers are more difficult for authorities to identify. For example, in Serbia, WhatsApp is used for home-based child prostitution.[56]

Gender based violence, including sexual abuse and sexual exploitation of girls and boys, engagement in prostitution, transactional sex, and forced marriage

Predators can use social media accounts to more easily identify people who need money and are therefore more vulnerable to exploitation. In this way, social media is an entry point for traffickers to abuse and exploit children for labour, trafficking, panhandling, and sex work networks.

References to personal payment accounts are common on social media profiles within online communities of marginalised groups, including women, people of colour, immigrants and LGBTQI-identifying individuals.[58] Young people in the US have been using online mobile payment sites like Venmo to raise money for costs they cannot manage, for example, to pay for family expenses when a family member is detained or deported by immigration.

Social media provides an easy way to contact and exploit children who are depressed or lonely, in difficult circumstances, or pushed to earn money in situations where they are not legally allowed to work, such as when displaced.[57]

Exploitation by policing authorities and increased risks of coming into conflict with the law and being perceived as criminals

US Immigration and Customs Enforcement (ICE) announced in 2017 that it would use artificial intelligence to evaluate a prospective immigrant's probability of becoming a positively contributing member of society. Data scientists raised alarms that this type of model would likely be biased and inaccurate, allowing ICE officials to arbitrarily flag certain groups or individuals under the guise of a supposedly impartial algorithm.[59] Multiple cases of ICE using social media and information gleaned by for-profit data brokers to track down and arrest immigrants have also been reported.[60]

Recruitment by armed forces and groups

In Greece, Save the Children staff reported concerns that social media was being used to radicalise vulnerable child and youth migrants.

Social media messaging and propaganda are specifically developed to draw in young people. Young unaccompanied refugees have been found to be more vulnerable to radicalisation if they have been separated from their parents. It has also been argued that refugee youth can become autonomously radicalised through online content.[61] This is sometimes referred to as 'weaponisation of information'.[62]

In El Salvador, for example, youth are bullied, threatened, and encouraged to join gangs via social media. If they refuse, they often feel obligated to migrate out of the country.[63]

4 Data misuse or mishandling

While digital inclusion helps fulfil children's rights to information and participation and helps them access vital services, an increase in digital inclusion means that a greater amount of highly sensitive data (e.g. biometric data, DNA and location data) is captured, which heightens risk.

Though there is great potential for drawing out insights from otherwise disperse datasets by combining and sharing data, this assumes good intent and good practice on all sides. When working with local and international implementing partners, donors, governments, and/or private sector organisations, there can be a lack of clarity about how to manage data sharing and who has responsibility. Furthermore, it can be hard to determine the extent to which children's data is protected and by which regulations when serving people from and across multiple countries.

Colin Crowley / Save the Children

Types of data that pose a greater risk of harm

Certain types of data may foster greater risk of harm or misuse. Agencies should have clear policies and risk-benefit assessments to guide their use of these types of identifiers, especially with children.

However, some aid agencies may lack awareness about how certain types of data can be used. There may be an assumption that encrypted, non-personalised data is anonymous, when in fact it is vulnerable to back-tracing and re-identification, or other kinds of misuse by more sophisticated actors.

Certain types of data may foster greater risk of harm or misuse. Agencies should have clear policies and risk-benefit assessments to guide their use of these types of identifiers, especially with children

In addition to anonymising or de-identifying microdata, agencies also need to think about how to de-identify or anonymise *aggregate* data and how to remove the association between aggregated data and groups of people. Organisations often access or share personal information of children based on a legitimate interest in providing services. However, the provision of these services does not always justify the risk or potential harm that might be caused by this data collection and most organisations do not have strong risk-benefit assessments in place to evaluate this. Types of data that are more sensitive and carry greater risk for children are outlined on the following pages.

Biometric data

Biometric data such as fingerprints, iris scans, and facial recognition are considered 'sensitive data' by the GDPR, meaning that a privacy impact assessment must be carried out before biometrics are used and special data protection needs to be in place if this type of data is collected. Biometrics are sometimes used to identify children in countries that do not have effective birth registration systems.[64]

Biometric identification can serve positive purposes, such as assisting in case management and family reunification, however, as biometrics are unique identifiers their misuse can result in serious harm. Biometric data can enable precise and private inferences to be made about the lives and exact movements of vulnerable people, which has serious consequences if governments of host countries or countries of origin request or demand humanitarian biometric data to repurpose for national security, immigration, or law enforcement.

Furthermore, facial recognition has been deemed a biased tool because of its differential rates of accuracy. When used with people who have light skin it is more accurate than when used with people who have darker skin. This leads to more cases of mistaken identification of darker skinned individuals, which is highly problematic when used by law enforcement or immigration agencies.[65]

UNICEF, Oxfam, and World Vision caution about or have placed bans (temporary or otherwise) on the use of biometrics.

DNA

DNA is another way to uniquely identify individuals and provide personalised aid. A person's sex, medical history, future health risks, family relationships and more can all be gleaned from their DNA.

Like biometrics, DNA is an invasive, permanent unique identifier that if drawn from children can lead to life-long privacy risks and implications. For example, DNA data can be used as a basis for tracking and targeting.[66] The extensiveness and intrusiveness of DNA testing means that most agencies avoid using it for routine operations, due to the privacy risk of collecting more personal data than is needed for a particular task, and UNICEF does not recommend collecting it.

Marieke van der Velden / Save the Children

Location data

Location data can provide helpful information for displaced and migrant populations, for example, the International Organization for Migration (IOM) created an application that provides location information for shelters along the migration route from Central America to the United States.

However, the risk of location data being misused by governments or other groups to track and trace individuals is a concern. Young people and their families were reportedly concerned that the IOM application could make them a target for those who could cause them harm (e.g. smugglers, local armed groups or thieves) because the location of the shelters could easily be found online. Families preferred to use a handkerchief that the Red Cross has provided, with a map of shelter locations on it.[67]

During the Ebola crisis in 2016, issues were raised when cell phone data records were released to aid agencies by several governments, to be used for contact tracing. It was unclear whether digital contact tracing could be effectively used to stop the spread of Ebola, or whether the opening of private cell phone records unnecessarily revealed personal data.[68]

The COVID-19 pandemic also brought this issue to light when 'contact tracing' apps were proposed in many countries around the world. In this case, mobile location data (through Bluetooth or GPS) would allow individuals and in some cases, governments, to identify when an individual had been within a certain distance of another person who had tested positive for the virus. Pushback was widespread and their efficacy was deemed by many to be insufficient to legitimise the amount of data they would collect. Fears about other potential uses of this data were also raised, especially as private sector companies who are known to collaborate in surveillance work with governments were involved.[69,70]

Thomas Jepson-Lay / Save the Children

Anonymised and de-identified data

Anonymised and de-identified data puts people at less risk because it has been scrubbed of identifying information or aggregated to a level where individuals cannot be identified. The process of removing personally identifiable data from microdata in order to make it anonymous is referred to as data anonymisation, or data de-identification.

However, anonymised data can still pose risks to individuals. Even if they cannot be identified from a particular microdata file in isolation, it may be possible to re-identify individuals using (statistical) matching with other datasets. Because of the volume of data that is now being collected (directly and indirectly) about people and because datasets are often combined and merged, it is becoming much easier to identify individuals within datasets.

Metadata

Metadata provides information about other data, for example, the date, time, geolocation and camera settings that are stored within a digital photograph, or the sender, receiver, date and time sent, sending and receiving server names and addresses that accompany an email. Metadata about mobile communications can reveal all kinds of information, such as a person's position and movements.

Metadata from social media and mobile phone records have been used to map social connections between individuals. Even when the contents of transactions are encrypted, data about these transactions is not. It is therefore possible to piece together online activity that reveals the physical presence of the person engaging in that activity.

This means that metadata can be used to track, target and retaliate against individuals and groups. Some governments, for example, are using data gathered from asylum seekers' smartphones to verify claims made in their asylum applications.[71]

Group data

Group data has been paid less attention than personal data; most data legislation focuses on protecting personal data at an individual level. However, individuals are often grouped together based on particular demographics such as ethnicity, religion, genetics, affiliation with a particular political group, or a shared geolocation such as a village or community. Many emerging data approaches developed by the private sector for marketing and political micro-targeting are aimed at creating groups of similar individuals in order to profile them, normally for advertising or behaviour change communications that nudge a particular group towards a certain political opinion or behaviour.[72]

Even if an individual is not specifically identified within a group, an individual can still be subject to harms because of their inclusion in group data, even when the data is anonymised.[73] Risk can emerge even when not using sophisticated data techniques such as profiling. One organisation, for example, geo-located children's school routes in order to visualise how far children travelled to attend school. This grouping and geolocation of where children congregate and where they walk to school could put them at risk of harm or violence or harassment from armed groups.

Potential for misuse or mishandling when collecting and sharing data

Here we examine five key areas where there is potential for data misuse or mishandling as a result of collecting and sharing children's data.

A Data sharing with private bodies or governments

Governments, immigration and law enforcement entities, and the private sector may intentionally engage with aid agencies in order to profit from or target specific populations through agency-collected data.[74] Some individuals involved in developing shared data bases have questioned whether the potential risks overshadow the benefits and whether there is currently sufficient critical thinking in the child protection sector on this issue.[75]

Refugee or migrant population data should not be shared with governments, militia, or non-state actors who may see them as targets for persecution, arrest, or deportation. For example, data of a child who was formerly a member of an armed group should not find its way into the case load of a government official who would use that information in a way that could harm the child.

Private companies have been known to advertise their services to child protection agencies and humanitarian organisations, while at the same time they provide digital investigation services to government agencies to track and apprehend refugees and migrants.[76]

Using data to identify and track people for deportation

Privacy International notes that several data and analytics companies have avoided scrutiny about their role in feeding data into ICE's data bases. Datasets provided to ICE by private sector companies include electoral registers, the census, local, state, and national online newspapers, sex offense registries, web cookies, email trackers, smartphone apps and third-party trackers, companies people interact with online and offline, social media sites, online quizzes, surveys, prizes, financial companies, other data companies, and many other sources. The data and analysis systems that these companies sell to ICE are used by the agency and others to identify and track people and their families, for purposes including deportation.[77]

Potential risks of collecting sensitive information from refugees

After conducting research and country case reports for UNHCR, Privacy International raised a number of potential harmful scenarios resulting from agency collection of sensitive information from refugees:

1. UNHCR shares an individual case file with the national immigration and border control authority of the country of asylum, leading to the detention of family members in the country of origin.
2. A young refugee forced into a sexual relationship contracts HIV. This information is transferred to the local government authorities because of health data-sharing requirements. It leads to a forced return to his/her home country where he/she is stigmatised or killed.
3. UN agencies and implementing partners access a list of the names and geographic locations of individuals in a camp, in order to distribute aid more efficiently. The provenance of the data is lost, and errors go uncorrected in the shared datasets. Over time, it becomes impossible to identify all the places where the data resides because organisations continue to share it. A laptop with the data on it is stolen, and it is impossible to identify the nature or degree of the risk.[78]

Pim Ras / Save the Children

When large datasets of refugees, migrants, and asylum seekers are handed from aid agencies to governments it creates risks and concerns, too. Core to this is the question of trust. In one case, it was reported that a UN agency handed over datasets of refugees and migrants to a host country government. It is unclear whether this actually happened, but the mere rumour caused stress and anguish to refugees and to agencies who did not agree to sharing datasets containing refugee identities, including biometrics.[79]

The advent of COVID-19 has brought this type of conundrum to the foreground, as humanitarian cash transfer programmes are running in parallel with government social protection programming, and governments are requesting that aid agencies share lists of cash transfer beneficiaries. Data sharing with governments can erode trust between implementing partners and large agencies, and it can also make refugees and migrants resist being registered and afraid to access services.[80] A study with Syrian refugees found that humanitarian aid workers and local government officials ranked lowest in terms of who they trust.[81] Another study reported that 33% of refugees had been asked to provide personal or sensitive information about their family or situation that they wish they had not given.[82,83]

Going even further, children's data can be used to target them as consumers, despite regulations in many countries which prohibit this. Children's private worlds are made visible to private sector actors with commercial interests who use artificial intelligence and algorithms to watch and record what a child is doing online, and then profile the child and manipulate the online social environment in ways that impact the child's sense of self, social networks, and social world.[84] If Save the Children is not aware of the risks or allows the private sector to dictate what data is captured, how it is used, with whom it is shared and for what purposes, the organisation will become unable to mitigate risks and harms. We need clearly stipulated agreements to ensure accountability.

B Misguided or involuntary consent

Consent requires a person or group to be truly informed. The complexity of new technologies leads to uncertainty about whether affected populations fully comprehend the technology, information flows, or the risks and benefits of allowing the collection and processing of their data.[85] The power dynamics involved could make people feel pressured to give aid agencies the data they ask for, which might not represent true consent in some contexts.

Establishing when there is a legitimate interest, and when there is not

The ICRC deliberated for a year and a half on the kinds of safeguards that would be needed to enable biometrics to be collected and used responsibly. It determined that consent was not a valid option when the provision of aid was contingent on a person providing their biometrics.

In the end, the organisation was able to establish a legitimate interest for the collection of biometric data in one case: for reuniting families or determining the whereabouts of missing persons, because this work is in the public interest and part of the ICRC's mandate as a global humanitarian organisation.

However, the organisation was not able to prove that it had a legitimate interest for collecting biometrics in a second case: beneficiary management and aid distribution. This was because biometric data collection in this second case was aimed at improving efficiency and was not absolutely necessary for distributing aid, which has been distributed for decades without using biometrics. Because biometrics were not necessary for aid distribution, the ICRC had to determine whether its legitimate interest in establishing a biometric identity management system outweighed the potential harmful effects on the rights and freedoms of the people whose biometrics would be captured.

Conducting this assessment to weigh the ICRC's legitimate interests in collecting this data versus the potential risks to beneficiaries' rights and freedoms helped the ICRC to identify different options for managing its biometrics program. In the end, the ICRC revised its biometrics system and found a way to balance its interests in collecting this biometric data with its need to protect the data privacy of beneficiaries.[86]

In the US, a pilot programme implemented by the Department of Homeland Security collected DNA profiles from migrants in immigration custody, including children. DNA samples were collected via cheek swabs, and biometric information was used to create profiles in a national criminal database run by the FBI. Officials stated that refusing to consent to DNA collection would result in a person being referred for criminal prosecution. Officials recognised in their privacy impact assessment, *"…several risks that have been raised by advocates, including the possibility that migrants would not know they have to consent to have their DNA collected or that some detainees, particularly children, could be unaware that the information would be sent to the FBI in perpetuity."* To partially mitigate these risks, notices were posted in ICE facilities and Customs and Border Patrol officers were required to give verbal notice.[87]

C Enforced trade-offs between sharing data and receiving vital support

To enable child protection work, agencies need to collect highly sensitive information about children that governments and companies around the world are restricted from collecting. Precisely because aid organisations are handling information that is deemed too sensitive for governments or corporations to have access to, those aid organisations have a greater responsibility to guard that information well.

People seeking services or shelter as a refugee, displaced person or migrant are used to providing their personal information in return for vital support and services.[88] The trade of personal data for services is not a new ethical dilemma, as a long tradition of research ethics shows. Yet the nature of the digital sphere and new ways that data can be captured and managed have brought this dilemma to the forefront for further review of the ethical aspects that should be considered.[89] When data is shared with governments in contexts where the government is actively denying the rights of certain populations, this becomes even more complicated.

D Varied legal frameworks across countries complicates multi-country programming

Technological capacity, language differences, network capacity, digital awareness, and varying legal frameworks all mean that what is designed and developed in a headquarter setting may not translate well to a local setting.

The digital space moves more quickly than national legislation. This is why agencies need to develop policies and practices that are agile and flexible enough to adjust to changing realities, and cover areas that do not yet have clear legislation.

Overall, the sector is moving toward more localised data privacy and protection policies. Much of this movement has been spurred by the GDPR and a growing recognition of the need to better manage digital data both to protect vulnerable groups and to avoid fines and legal action. Many European and UK based aid agencies, including Save the Children, developed new data protection policies in order to comply with the GDPR, which came into effect in 2018.

By 2020, 132 of the world's 194 countries had put data privacy and protection legislation in place or were in the process of doing so.[90] Many of these legal frameworks mirror the GDPR, however some introduce new definitions and concepts. This complicates multi-country programming because it is difficult for organisations to reconcile the various legal frameworks related to the treatment of data. For example, the US, the EU and India use different definitions and define data categories slightly differently, which makes it difficult to harmonise orientation and guidance at a global level. It is a challenge for global organisations to keep track of the various laws that dictate how they should collect, manage, share, and store data.[91]

In the absence of a consistent legal framework, policies often cannot provide answers to questions about what to do in conflicting legal situations. In the aid sector, agencies often implement programmes across multiple countries, with people from multiple countries. Clarity on who has which legal rights, and who is covered by which regulations is difficult to parse. This was identified by some of the people who were interviewed for this report as the aid community's biggest blind spot. Ability to access and use data is often found in countries with less democratic governments where there are weak legal and civil protections, and governments are able to use sophisticated surveillance tools to target and harm specific groups.[92]

In addition to this challenge, the digital space moves more quickly than national legislation. This is why agencies need to develop policies and practices that are agile and flexible enough to adjust to changing realities, and cover areas that do not yet have clear legislation.

E Lack of child focused data privacy laws in host countries

Several countries have specific legal frameworks covering children's data and because organisations are required to follow the law, agency policies have been impacted by these legal frameworks.[93,94]

However, many refugee hosting countries do not have privacy or data protection laws or authorities to enforce them. Even if an agency working with refugees has its own guidelines on how it manages personal data, refugees have the duty to conform to the laws and regulations of their host country.[95,96]

When it comes to children's data protection in particular, not all country legislation defines specific obligations towards child data subjects. Governments can find large amounts of personal data about children online. This type of surveillance was largely unimaginable in the pre-internet era, and is often not lawful or publicly acknowledged, however, it forms a key part of national security. Not only does this undermine basic notions of privacy, it threatens human rights, including freedom of expression. It also opens the door to potential abuses of state power.

National laws and international documents are largely based on principles of parental consent for capture of children's data. Consequently, there is no adequate protection for children's data privacy rights in situations where data is accessed from these new sources.[97] The full implications and potential outcomes are not fully understood, but if governments can link individual profiles with data captured through mass surveillance, authorities would be able to build and maintain records of children's entire digital existence.[98]

Lack of child-specific privacy laws raises serious concerns for children's safety; for example, a displaced child who was previously a child soldier could come under the digital scrutiny of the government that he was once forced to fight, or a child with irregular migration status could be found through a Facebook post and subsequently location tracked and apprehended by authorities

Children's data used to track undocumented family members

In the US, children's data has been used to track undocumented family members. The agency tasked with caring for children separated from their parents at the US-Mexico border shared information on US-based relatives and potential sponsors with the Department of Homeland security.

The information obtained from detained children who were trying to find family member was used to arrest and deport these family members. The result is that *"families have become too scared to step forward to sponsor children"* and *"children are being turned into bait to gather unprecedented amounts of information from immigrant communities."*[99]

How is Save the Children addressing digital safeguarding?

Save the Children is a sector leader in child safeguarding and child protection. The organisation has robust child safeguarding and child protection policies, and an abundance of research and practical guides for programme implementation available internally and externally via the Save the Children's Resource Centre.[100] Save the Children offices are highly active in child online protection programmes, advocacy and policy, and the organisation has been recognised by the UK Charity Commission for its work on child safeguarding, child protection and risk management, and praised for its incident reporting and case management systems.

In order to better understand how Save the Children's existing strengths extend to child safeguarding in the digital realm, internal documents were reviewed and almost fifty interviews were conducted with staff from Save the Children offices, including international headquarters (the Centre), three member offices (US, Denmark, Switzerland) and five country offices (Lebanon, Ethiopia, El Salvador, Afghanistan and The Balkans).

Pim Ras / Save the Children

The organisation has a solid base upon which to build a more robust digital safeguarding effort. Consultations with stakeholders indicated that Save the Children staff have very high awareness of safeguarding and child protection. Staff across all offices said that "safeguarding is everyone's job." There appear to be strong levels of critical thinking related to the introduction of digital devices and new and emerging technologies in programming and a deep concern for ensuring that digital technology and innovation are not harming or excluding children. Safeguarding is a core thread that runs through the organisation from the beginning to the end of programming, and from the bottom to the top of the organisation. Child safeguarding and data security policy and practice are generally strong, and staff are regularly trained on both. Communications and social media policies are also well-developed, and staff are aware of these and in most cases work to implement them. Addressing specific gaps in digital and technology knowledge, policy and orientation or guidance, as listed throughout this report, would help improve digital safeguarding practices and help staff to feel more confident in their safeguarding and safe programming efforts, and this would help the organisation to innovate more confidently.

Below is an overview of Save the Children staff awareness on digital safeguarding risks and what existing policies or practices are in place internally to address the four areas identified in our risk typology.

1 Exclusion and self-exclusion

Save the Children staff who were interviewed were very aware of the digital divide and lack of digital access of many of the most vulnerable children with whom the organisation works. Save the Children is involved in some programmes to provide devices or educational materials to children to make up for this lack of access (e.g. Child Online Safety Centres in the North West Balkans). Staff across the organisation are quite aware of how literacy, language, economic status, age and sex/gender can contribute to reduced digital access. Generally, programmes are designed with the community in mind and the idea that devices must be accessible by communities working with Save the Children.

Save the Children's involvement in online safety and other child protection programming has also increased awareness among staff around issues of online bullying that might lead to self-exclusion, according to some staff who were interviewed. Save the Children staff in the Balkans were especially aware of the need to build trust among young people if desiring them to use digital applications or provide data. In Afghanistan, staff spoke extensively about the need for community engagement and local risk assessments before introducing technological devices or online data collection, because use of these devices can raise the organisation's profile among armed groups and put anyone involved at risk.

Areas to strengthen

Save the Children's approach to its work is inclusive and consultative. The organisation could, however, benefit from regular, localised research on the kinds of devices, platforms, communication channels and media sites that migrating and displaced children in different contexts are using, because this changes quickly and regularly. Staying on top of the shifts in technology and children's use of it would help the organisation to ensure that it is not excluding children when designing digital programming and communications. As part of this work, Save the Children should explore issues of trust in digital technology as well as in different agencies and the wider sector, attitudes to privacy, and online experiences of children on different platforms so that reasons for self-exclusion can be better understood.

2 Harm caused by humanitarian innovation

Among some staff, there is concern that Save the Children could become a conduit for humanitarian innovations taking place in a deregulated environment. As one staff member said, *"people don't think about future uses and applications of technology that we don't yet understand. We tend to conform to the sector standard. But what about long-term repercussions of some of these approaches?"* According to some staff, this conformity in the sector occurs because of competition for funding and at times, donor demand. It can be hard for staff at lower levels within the organisation to push back when potentially unsafe or risky innovations are included in funding proposals.[101]

Risk assessments do not systematically include specific questions about innovative approaches, data, or digital technology. Rather, it appears that it is up to individual teams to incorporate this in their risk assessments. Save the Children programme offices have varying degrees of technical expertise with emerging technologies and the kinds of data protection issues that arise with newer technologies and platforms, or with newer data approaches that go beyond traditional data collection and processing. Power dynamics between donors, the private sector, and across different Save the Children offices could also mean that risky programmes or practices are allowed to move forward if they are seen to bring benefits such as funding or a higher profile.

Though most staff across Save the Children offices consulted said that all proposals are reviewed before submission in order to identify and mitigate potential child safeguarding issues, not all staff felt confident that emerging digital safeguarding risks were sufficiently explored, and in some cases the process for review of new initiatives or proposals is not entirely clear. Staff working in fundraising for innovations mentioned that there is an ethical review board for public health programmes and an ethics review committee, but they were unsure whether these forums consider digital or online safeguarding. Staff also raised concerns that the risk assessment process is not institutionalised or systematic enough and that there is insufficient expertise and training to assess innovations, emerging technologies, and new kinds of data capture and use.[102,103] In the past, Save the Children risk assessments have focused on safety and security, child safeguarding, construction risks, and medical/pharmaceutical risks.

Save the Children has not yet incorporated risk analysis related to innovation, new types of partnership, data sharing, and emerging technologies into its risk assessment process

Save the Children has not yet incorporated risk analysis related to innovation, new types of partnership, data sharing, and emerging technologies into its risk assessment process. The process is designed to take direction from country offices on key risk areas, yet some ethical considerations relating to public-private partnerships, innovations, and the use of data are emerging that need to be flagged and addressed at an organisational level.[104]

The lack of an overarching ethical framework coupled with limited capacity and innovation and digital expertise, exposes children as well as Save the Children and its partners to risk. Additionally, there is insufficient attention to evaluating the impact of new technologies in Save the Children's programmes. As one staff member noted, *"there's a lot of interest in the organisation around being innovative and using more tech tools. We're seeing more benefit from technology that helps projects become more efficient or scale up than we are from tech that actually benefits our beneficiaries. I'd love to be able to say the kids are better off, but there's not much evidence of that."*[105]

Areas to strengthen

Save the Children should put a more systematised and institutional approach in place for assessing and mitigating risks in this area, including a multi-disciplinary review board and well-informed legal counsel. Having stronger, more structured systems and capacities in place for reviewing digital safeguarding and assessing potential risks as well as measuring benefits of innovation and technology would allow Save the Children to feel more confident about entering into new or innovative programme areas and using emerging technologies in its programming. As Save the Children empowers its local offices and staff to make decisions about which risks need more focus, additional training and capacity is needed so that staff are confident they have the knowledge, skills and support to make those decisions. With new and emerging approaches, if left to individuals, it is possible that people *"won't know what they don't know"* and this could lead to harm.

Furthermore, development of research, monitoring, and evaluation frameworks will allow the organisation to identify and address short- and long-term benefits, risks and harms from experimentation and innovation.

3 

Increased exposure to online harms

Use of social media platforms, apps and the wider internet – whether actual or aspirational – are a part of children's worlds. Newer digital communication channels have great potential for Save the Children's work, and COVID-19 quarantines have meant that staff are now relying more heavily on them to reach community members, partner organisations and children. The digital world is known for its unpredictable shifts in trends and habits, and organisations often struggle to keep up to date with their online protection measures. The challenge is how to help children and youth take advantage of what digital technologies can offer while supporting them to engage safely with digital platforms as part of Save the Children's programmes and in their private lives.

Overall, Save the Children staff appear to have a very high degree of awareness of the benefits and the potential risks that arise when children use the internet and mobile phones on their own, and when Save the Children introduces devices or digital channels to children or uses digital platforms, tools or social media channels in its work. Several interviewees from different parts of the organisation mentioned that they are involved in online child protection programming, and most staff also mentioned that they conduct risk assessments and risk maps when embarking on programmes that would expose children to the online environment.[106,107]

Preventing online exploitation and violence in the Balkans

In the Balkans, Save the Children is implementing a project to prevent sexual exploitation and violence against children in the digital environment. This involves working with the police; specialised training on tools and software to detect online abuse; working with schools to develop specific curricula to raise awareness among children about how they can protect themselves; and advocacy for legislative solutions.

The programme includes NGO and institutional partners, who are working to change laws in the area of social networks[108] and the Save the Children office in the Balkans has also conducted research on this topic.[109] Ten Member offices are working on online child protection in their national programmes as well as globally.[110]

Strong social media policies guide staff on aspects like consent for photos and stories in communications work, identity protection and management of children's images, and prohibitions on having direct contact with children through social media. Staff frequently mentioned the social media policy when asked about organisation child safeguarding policies.[111]

Children who are migrating or displaced or who have come from situations where they have been exposed to violence and conflict, may consider images that other people find shocking appropriate to share. This makes it difficult to know when staff should step in.[112]

Save the Children uses children's images and stories to support fundraising and advocacy, but these can open children to abuse when published on social media or other channels. Again, there is a clear policy for this area, yet Communications staff reported that consent to use images and stories is a constant challenge. Anonymous photos are less risky, however they are also less engaging and effective for fundraising or advocacy. Staff follow designated consent processes but find them challenging when a child does not want to have their photo used but feels that they owe it to Save the Children in return for benefits they access through the organisation's programmes.

Save the Children

It is difficult to know if people understand how their stories and images will be used and where they might end up. Children, parents and guardians often do not know the difference between 'Facebook' and 'social media.' They may consent to their images and stories being posted on social media but retract their consent when they realise that this includes Facebook.[113]

Staff in a few country offices said that Save the Children's strong, strict policies on social media do not work well for small partner organisations who lack the staff, knowledge, capacity, systems, and budgets to meet Save the Children's standards.

Areas to strengthen

Save the Children needs to update, localise, and contextualise its online child protection policies as newer technologies come into play, and as children increasingly use these devices and platforms unsupervised by organisations or caretakers, as is often the case with migrating and displaced children. This should be an area of ongoing research and investment. Updated and contextually specific digital safeguarding policies are also needed both for Save the Children and for partner agencies that can address differential risks and risk factors according to the life experiences of children and to local resource levels and capacities.

Save the Children needs to establish a regulatory framework with partners, which ensures they have the capacity and technological understanding that is required. Staff also requested additional guidance on how to develop a Memorandum of Understanding with partners who are providing devices (e.g. to cover issues such as software that would block inappropriate websites, inappropriate content, monitor use of tablets), and additional orientation on Save the Children's obligations, and those of beneficiaries and partners.[114] This is particularly important given the greater focus on localisation and the implications of COVID-19, where there has been an increased reliance on local partners.

Even with strong policies, it is difficult for staff to assess the potential benefits and risks of digital channels. According to many staff, Save the Children's social media policy should be reviewed and updated to better reflect the reality of social media use in programmes, operations, and among children and young people. It should be more contextually relevant, flexible enough to adapt quickly as platforms shift and change and as children move from platform to platform, and it should help staff to navigate competing risks for children. It may be that there are not always hard and fast rules, and that mechanisms to access guidance for different situations, sometimes on a case-by-case basis, are needed.

4 

Data misuse or mishandling

Save the Children has strong data security protocols that are centralised and organisation wide. These include device registration and encryption, multi-factor authentication for laptops and mobiles, remote wipe, use of cloud storage and SharePoint (file storage that staff can access remotely), internal file sharing via One Drive, access control to data and systems, anti-virus software, and IT policies and procedures such as data privacy and confidentiality clauses and data sharing agreements in contracts and partnership agreements.[115]

Across all offices, staff mentioned a wide range of data protection policies and practices. Staff look to IT teams to keep them up to date on data security issues, social media, and digital communications.[116] Countries use a safeguarding information management system called DATIX for centrally managing child safeguarding cases. Concerns are reported online, and the system automatically notifies relevant persons at country offices, regional offices, and globally. Follow-up is managed through the system.[117] Countries who implement child sponsorship also have a protected database for managing child sponsorship data.

Digital case management for child safeguarding and child protection is inconsistently implemented … this has given rise to inconsistent management of child safeguarding.

In 2017, Save the Children International began rolling out a data protection policy in order to adhere to the EU's GDPR,[118] which is considered the world's strongest data protection framework to date. Training has been provided across offices, which have been encouraged to adapt the data protection policy to their local context and legal environments. The GDPR was a catalyst for Save the Children to implement more data-related policies and procedures.[119] While Save the Children's global IT and data protection policies are strong and aim to comply with the most stringent data protection regulations, there are still gaps in implementation and contextualisation when it comes to how different offices are capturing, processing, and sharing data. Staff from Save the Children International noted that data protection is still a nebulous concept for many within the organisation. According to staff from Save the Children UK, an initial attempt to create global training was overly influenced by UK legislation and too complex, with an abundance of legal language. A second attempt at global training is in the works, which will be more suitable for non-native English speakers. The organisation is also still working on the application of policies at the country office level.[120]

Digital case management for child safeguarding and child protection is inconsistently implemented. Save the Children is one organisation, yet it works as a Federation. Save the Children International directly manages country offices but does not have jurisdiction over its Member (fundraising) offices. This has given rise to inconsistent management of child safeguarding depending on whether Save the Children International or Save the Children Members are involved.

There appear to be good data management practices in country offices (e.g. password protected files, data deletion when a case is finalised) but this might be an area to explore further to ensure that staff have the tools they need and that those tools are consistent and secure. DATIX is also not aligned in some cases with local processes, as noted by a few offices. This leads staff to create shadow systems (for example, Excel spreadsheets) that are less secure in terms of data privacy and protection.

Technology is also being trialled for digital child protection case management data systems to assist teams and social workers. Again, there is inconsistency across the organisation in terms of which systems are being used and the trust that staff place in them. Some staff are highly engaged in implementing them, while others have concerns that data within the systems will be shared with government, and some doubt that the systems will work and have created their own simplified applications that they consider to be a better fit for their context. For example, in the Balkans, staff said that children often give false names and false birthdays due to lack of trust, making it difficult to track anyone, even for beneficial purposes.

Areas to strengthen

Save the Children staff appear to be very aware of data security and have a strong centralised approach. They know about privacy risks but recognise that this area has not been addressed in the same cross-institutional way that other kinds of safeguarding have, and there is insufficient knowledge and capacity around emerging kinds of data privacy and protection risks.

The complex nature of data capture, processing, and sharing means that it is less easy to assess potential risks. Gaps here include awareness, training and resources. There is a need for point persons to help move better practices through the wider organisation. Save the Children is not alone in this and could benefit from developing good practice guidance and embarking on capacity building in collaboration with the wider sector. As noted with regard to the risks of experimentation and digital innovation, staff "don't know what they don't know", and this can lead to insufficient capacity to identify and mitigate risk.

Staff at a few country offices said that they would like to have practical data protection and management guidelines that are more contextually and operationally relevant. These policies need to be 'right-sized' for the local situation. Stable camps and more transitional contexts require different approaches, and heavy, ponderous systems will likely not be a good fit for staff needs.[121]

Additionally, local partners often do not have the capacity to implement complicated standards or the necessary IT systems to manage data securely. This becomes a challenge for Save the Children in adhering to its data policies and keeping children's data safe. The organisation has tried to avoid shifting risk to partners, but capacity building has a cost that donors are not always aware of or willing to pay for.[122] As one staff member said, *"it's important for us to advocate towards the donors to start recognising child safeguarding costs in project proposals…. We need financing for safeguarding, not only for Save the Children but for our partners."*[123]

Staff have specific questions about how to use data safely in specific scenarios. They have numerous questions and support needs over a wide range of technologies and contexts, but limited support is available. For example, staff interviewed for this report asked for additional support and guidance on data sharing with partners, re-use of community mobile phone numbers for secondary purposes during an emergency, use of WhatsApp for child protection case management in camp settings, setting up encryption on open source data collection applications, data ownership, data retention and deletion.[124]

In general, there are challenges with the use of photos of children. Although there is a policy for this, staff in some offices asked for specific guidance for managing photos captured on personal devices and sharing stories and photographs of displaced or migrating children. Some are worried that donors might be able to re-identify children who are featured in case studies if they share photos and stories on their own websites or social media pages. There is plenty of guidance, but it is a challenge to put it into practice and not all guidance seems to address the vast range of issues that may arise.[125–127]

The aid sector's approach to digital safeguarding

Save the Children's 2019 study on displaced children and emerging technology[128] recommended a more institutionalised policy and practice to reduce the potential for harm from digital innovations and digital programming. Alongside a primary concern about risk to children is a concern about compliance and legal risks to organisations, considering new regulations on data privacy and protection emerging in several countries around the world over the past few years. As the aid sector's digital programming grows, and as the adaptations and restrictions necessitated in response to COVID-19 continue, the impact and scale of these risks are likely to grow.

Alongside a primary concern about risk to children is a concern about compliance and legal risks to organisations

A comprehensive review of existing operational and academic research, legal frameworks, grey literature and aid sector guidance documents revealed only a few resources addressing the specific intersection between children or child safeguarding and digital programming or innovations (see Annex 2 for a list of documents reviewed). None of the documents addressed digital safeguarding holistically and specifically in child migration and displacement contexts. There are, however, several documents that include some aspects of guidance and good practice. Consequently, to gain additional insights into how the sector more widely is addressing child safeguarding issues related to use of digital technologies, 12 key informant interviews were conducted with external experts identified through the literature review. Existing policies helped to identify five considerations for effective digital safeguarding: inclusive programme design; due diligence and risk assessments for innovative partnerships; online child protection guidelines; non-traditional data management guidance and governance and accountability procedures.

Inclusive programme design

Inclusive programme design can help agencies to better understand the digital environment and context so that programming does not exclude children who cannot access the digital environment or who are not represented in datasets.[129] Some existing guidance provides orientation on conducting research about how children access and use digital devices and the internet.[130]

Additional guidance on conducting programme design and risk-benefit analysis would be beneficial in order to identify areas where self-exclusion might occur. Programme designers can then address those issues before implementation begins.[131] This would include orientation on design research to understand children's access and habits, which existing sites and applications they feel are safe, which organisations and entities they trust or do not trust, and why (see safe research section of Girl Effect's Digital Safeguarding Tips and Guidance).[132] Better policy and guidance for vetting partnerships, as outlined in the section on safer online and social media experiences, protection of data as well as institutional data governance and greater accountability would all contribute to mitigating exclusion and self-exclusion.[133]

Due diligence and risk assessments for innovative partnerships

Very few policies ask 'big picture questions' about the ethics of humanitarian innovation. For example, what might be the long-term impacts of introducing a particular technology or a new approach? If disruption is the goal, who is being disrupted and what might the implications be? Staff might be aware that they need to protect data, but they neglect to ask the important first question: should we even be doing this? Over the past five years, the humanitarian innovation space has begun to focus on how monitoring, evaluation, and learning can support more responsible innovation. This has come from a recognition that innovations can create harm in a number of ways, as well as bring benefits.

Very few policies ask 'big picture questions' about the ethics of humanitarian innovation. Staff might be aware that they need to protect data, but they neglect to ask the important first question: should we even be doing this?

Policies and procedures could help to address the upstream implications of potentially harmful technology that stem from innovative partnerships with the private sector. Missing from the policy toolkit is a due diligence process and a risk assessment of the potential benefits and harms (specifically to children) created by innovation partnerships. This type of guidance could help organisations consider the potential short and long-term implications of a partnership and document decisions about whether to proceed or not.[134] In the end, safeguarding and protecting children might be more about *not doing* something than it about *doing* something, suggested one humanitarian expert on ethics and innovation.[135] A 2018 academic paper categorised the risks of humanitarian experimentation as:

1. underlying trends and the risk of harm;
2. distribution of harm: ethical variability in humanitarian space;
3. resources distribution and scarcity considerations; and
4. legal liability and reputational damage.

The Response Innovation Lab (RIL) offers an Innovation Monitoring and Evaluation (M&E) Toolkit that covers prototyping, piloting and scaling, for example,[136,137] and the Principles for Digital Development offer guidance on designing digital programming based on existing good practice and past learning.[138] Neither of these considers children in particular. Girl Effect's 2018 guidance on digital safeguarding does include an initial set of questions about whether an initiative is ethical or a good fit and could serve as a starting point for developing this area further.[139] This would need to be adapted and updated to focus on migrating and displaced children.

Core humanitarian imperatives and principles could also serve as a basis for assessing risks of humanitarian experimentation:

1. do no harm,
2. humanity,
3. neutrality,
4. impartiality and
5. independence.

These would need to be reoriented towards practitioners and adapted to the lens of the migrating or displaced child.[140]

Online child protection guidelines

Online child protection has topped the list of concerns for many children focused organisations over the past several years. Plenty of guidelines exist for children; teachers, schools and extra-curricular activities; governments and industry, aimed at improving online safety for children.[141–144] Save the Children created the Keeping Children Safe Online guidelines for organisations in 2014, in consultation with other child focused organisations[145] and released an Operational Handbook for Child Online Safety Centres in 2019.[146] Agencies are also starting to release specific COVID-19 related guidance for keeping children safe during a period where they might be online more often, due to virtual schooling and quarantines.[147,148]

Child protection has become more complicated in the online environment, for example when a child discloses in an online space that they have been abused. Agencies are not always well prepared to handle disclosure, especially if a communications or digital team is running the website and they do not have a child safeguarding protocol already in place. Signposting to local services is also challenging given the global nature of the internet and the aforementioned data protection risks if location data is collected from children. Girl Effect's Digital Safeguarding Tips and Guidance provides orientation for handling online disclosure, signposting, setting up online reporting protocols, recommendations for creating safe and healthy communities, and suggestions on community moderation online, but handling these types of cases continues to be problematic for the sector.[149]

Non-traditional data management guidance

A few documents specifically address responsible data management for children, digital data and technologies, and cover some aspects of migration and displacement contexts, but none are specifically designed to digitally safeguard migrant and displaced children.[150–154] Other documents cover children and the digital world, but do not specifically include the migration and displacement context.[155–158] Quite a few policies and related documents consider data management at aid agencies. Many of these mention children in terms of consent or recognise the sensitivity of children's data, but they do not go into detail or treat children and their data holistically.[159–163] Policy and guidance documents on data management during an emergency or crisis context also exist, but again these do not specifically focus on children and their data.[164–171] This is an area that is still developing, and there are no child focused agencies at the forefront.

Few documents specifically address responsible data management for children, digital data and technologies … to digitally safeguard migrant and displaced children.

The majority of agency policies and guidance on data protection address traditional, linear types of data collection and use, where an agency or its partners collect and manage data themselves. They do not address how agencies could or should access and use non-traditional forms of data such as big data or datasets collected or provided by the private sector (e.g. mobile phone data records from telecommunications companies or back-end data from technology companies). A concerning point is that only a few guidance documents[172,173] address the protection of demographically identifiable data, in other words, data that can identify a wider group of individuals and/or their location. Most policies and guidance have gaps in terms of ethics and challenges of data collected for predictive analytics, the use of facial recognition and biometrics, and the capture of location data.

There is also a lack of guidance on addressing the growing ease of re-identification of supposedly anonymised data through new methods or due to the so-called 'mosaic effect,' in which the combination of large datasets with different kinds of information about the same person(s) can allow people's identities to be inadvertently (or purposefully) revealed. UN OCHA is currently exploring this topic more in depth but has not yet produced guidance.[174]

There is a lack of clarity overall on how to manage data sharing and databases with local and international implementing partners, donors, governments, and/or the private sector.[175] Some organisations have major concerns about data security, especially at the level of local partners and frontline staff who may not have regular access to digital devices, to a secure or consistent mobile or Wi-Fi network, or sufficient bandwidth to use organisation-mandated tools and security protocols. In addition, while some organisations have focused on the threat of external hacking, addressing data breaches due to carelessness or poor security practices (such as sharing passwords or being infected by a virus or spyware) may be the greatest challenge.[176]

Data governance and accountability procedures

Policies often cannot answer the question of what to do in the case of non-existent or inconsistent legal frameworks across countries.[177] Contextual adaptation is a challenge for overarching digital safeguarding policies. Technological capacity, language differences, network capacity, digital awareness, and varying legal frameworks all mean that what is designed and developed in a headquarter setting may not translate well to the local setting.

Contextual adaptation is a challenge for overarching digital safeguarding policies. Technological capacity, language differences, network capacity, digital awareness, and varying legal frameworks all mean that what is designed and developed in a headquarter setting may not translate well to the local setting.

Additionally, it is often not clear to the external stakeholders we interviewed, who is responsible for which parts of digital safeguarding policy and practice, and what level of skill and awareness are needed across different parts of the organisation in order to comply with policy.

Language (most documents are in English), time, format, and capacity challenges create barriers to implementing data protection policies.[178] There remains an urgent need for better data governance and accountability at government, corporate and agency level. UNICEF is working on a Data Governance for Children manifesto that will advocate for greater protection for children's data, more ethical business models in the case of the private sector, and greater accountability from all sides. This might provide a basis for developing further guidance on accountability and governance.[179]

Within organisations, tensions can be found between innovation, business development, and fundraising teams on the one hand and child safeguarding, protection, and data privacy teams on the other.[180] Additionally, more work is needed to break down data protection and digital safeguarding materials from legal and technical language into digestible concepts that staff and partners can understand and implement locally and contextually.

Juozas Cernius / Save the Children

CONSIDERATIONS AND NEXT STEPS

Save the Children's firm foundation in child safeguarding puts the organisation in a strong position to move the digital safeguarding agenda forward. Save the Children should begin by strengthening its digital child safeguarding for migrating and displaced children and expand this to children overall, on the basis that building a policy around the most vulnerable will ensure the policy is as robust as possible. This kind of work cannot be done in a vacuum, especially considering that most programming and innovation will involve partners from the INGO sector, local organisations, government and the private sector. Therefore, a collaborative approach is needed to truly push forward this important work.

As there is currently no guidance specifically on the intersection between child safeguarding and digital programming and innovations, there is an opportunity for Save the Children to lead in this area. The guidance Save the Children will develop, on its own and in partnership with other organisations, needs to be flexible, adaptable to local contexts, and regularly updated so that it keeps up with the pace of digital change. Save the Children and other organisations should ensure that local partner organisations are supported with training, resources and other capacity strengthening efforts to ensure that digital safeguarding is adopted and embedded effectively.

The sector must strengthen its digital child safeguarding and safer programming for migrating and displaced children to ensure that the children we serve can benefit from the huge potential of digital technologies and be protected from harm. This study calls for the aid sector to ensure digital inclusion for all; establish greater trust in agencies; design clear innovation partnerships; ensure that digital programmes reflect beneficiary needs; increase digital literacy and capacity; provide clear ownership and governance and develop practical and consistent data management processes. An initial set of questions to guide a risk assessment across the four key risk areas outlined in this report, can be found in Annex 1.

Recommendations

1 

Ensure digital inclusion for all

The sector must broaden its efforts to improve digital inclusion and access for the most vulnerable children, including refugee and migrant children, because of the significant benefits digital inclusion can bring.

Agencies should invest in regular, localised research and consultation on the kinds of devices, platforms, communication channels and media sites that migrating and displaced children in different contexts are using to ensure that children are not excluded when designing digital programming and communications.

They should also ensure that children without smartphones or internet access are included in digital services or provided with alternatives. Identify ways to expand datasets and balance analysis to avoid skewed insights that are only representative of those with digital access; this will be context specific and might imply continuation of traditional data collection to ensure that the most vulnerable are included.

2 

Establish trust in the system

Lack of trust is a key barrier to children participating in digital programming, so ensuring that children's data is not misused by authorities, governments and the private sector is crucial in order to build their trust.

Further research on the extent to which a lack of trust in the system, agency or sector makes children reluctant to provide data may be useful. Exploration of additional barriers to data sharing among children would also be valuable to understand potential obstacles to participation in digital programmes and ways in which these could be overcome.

3 

Design clear innovation partnership frameworks

Development of research, monitoring, and evaluation frameworks will allow agencies to identify and address short- and long-term benefits, risks and harms from experimentation and innovation.

Agencies must put in place a structured process for assessing the risks that come from trialling innovations, including clear approaches for involving children and communities in design and risk assessments of any new type of programme. This is particularly relevant when working with partners to capture, process and/or share personal and sensitive data that could put migrating and displaced children at risk. To support this, training must be provided to ensure staff have the appropriate skills to carry out risk assessments effectively.

Mechanisms must be put in place to transparently share results and learning about innovations. Coupled with this, programme teams should establish a multi-disciplinary review board (including internal and external members), to review and approve experimental partnerships, partners, programmes, and processes for ethics concerns.

In addition, agencies should ensure legal counsel is available to guide any necessary agreements with innovation and/or digital partners and protect the interests of children and communities as well as those of Save the Children.

4 

Ensure that digital programmes reflect beneficiary needs and concerns

Participation and feedback from children and adults in local communities must be reflected in safeguarding policies, programming and advocacy work. Communities should be involved in the design and assessment of new digital programmes and their participation should be supported by the establishment of an ethical review board and clear channels for raising concerns and sharing results in a transparent manner.

5 

Increase digital literacy and capacity in the sector

Additional training and capacity are needed to give agency staff the confidence to deliver effective digital safeguarding at a local level.

Specifically, staff call for investment in:

- Orientation in how to develop a Memorandum of Understanding with partners who are providing devices, in order to fulfil safeguarding obligations.
- Updated and contextually specific digital safeguarding policies, which are needed as new technologies come into play.
- A regulatory framework with partners, which ensures they have the capacity and technological understanding.
- Clear, confidential, and accessible channels for raising concerns or complaints about new approaches, to be made available to children and communities, partners, staff, and others.
- Enhanced consent policies, which determine how to reconcile power imbalances in the consent process for more truly informed consent.
- Training and development of locally adapted resources, in various languages and easy-to-digest formats.
- Training focused on broad digital safeguarding concepts as well as more specialist areas such as risks with metadata, the potential for re-identification of anonymous data, and other emerging issues with data and data privacy.
- The continued roll out of data protection policies, with support given to offices to enable them to adapt policies to the local language and context, local data protection regimes, and local and global regulations.
- Specific guidance for managing photos captured on personal devices and sharing stories and photographs of displaced or migrating children.
- A review of existing social media policies and support to help local offices adapt them to be more contextually relevant.

Focal point contacts should be identified to help move better practices through their wider organisation and the sector, and to provide specific guidance on data privacy and protection questions in national contexts, as well as ways to manage conflicting legal regimens across countries.

6 

Provide clear ownership and governance procedures

A more systematised and institutional approach is required for assessing and mitigating risks, including a multi-disciplinary review board and well-informed legal counsel that can review as well as measure the benefits of innovation and technology.

In line with this, the sector must develop processes and guidance to build awareness that data protection is "everyone's job". Responsibility should not be reliant on one staff member to manage, maintain and update procedures or systems. This risks loss of key knowledge or information if an employee moves on. Agencies must collaborate to build sector-wide norms and training resources for staff and management on data and children, with a specific focus on migrating and displaced children.

Agencies must assess and update data governance and accountability chains to understand their effectiveness and budget for continual improvements.

7 

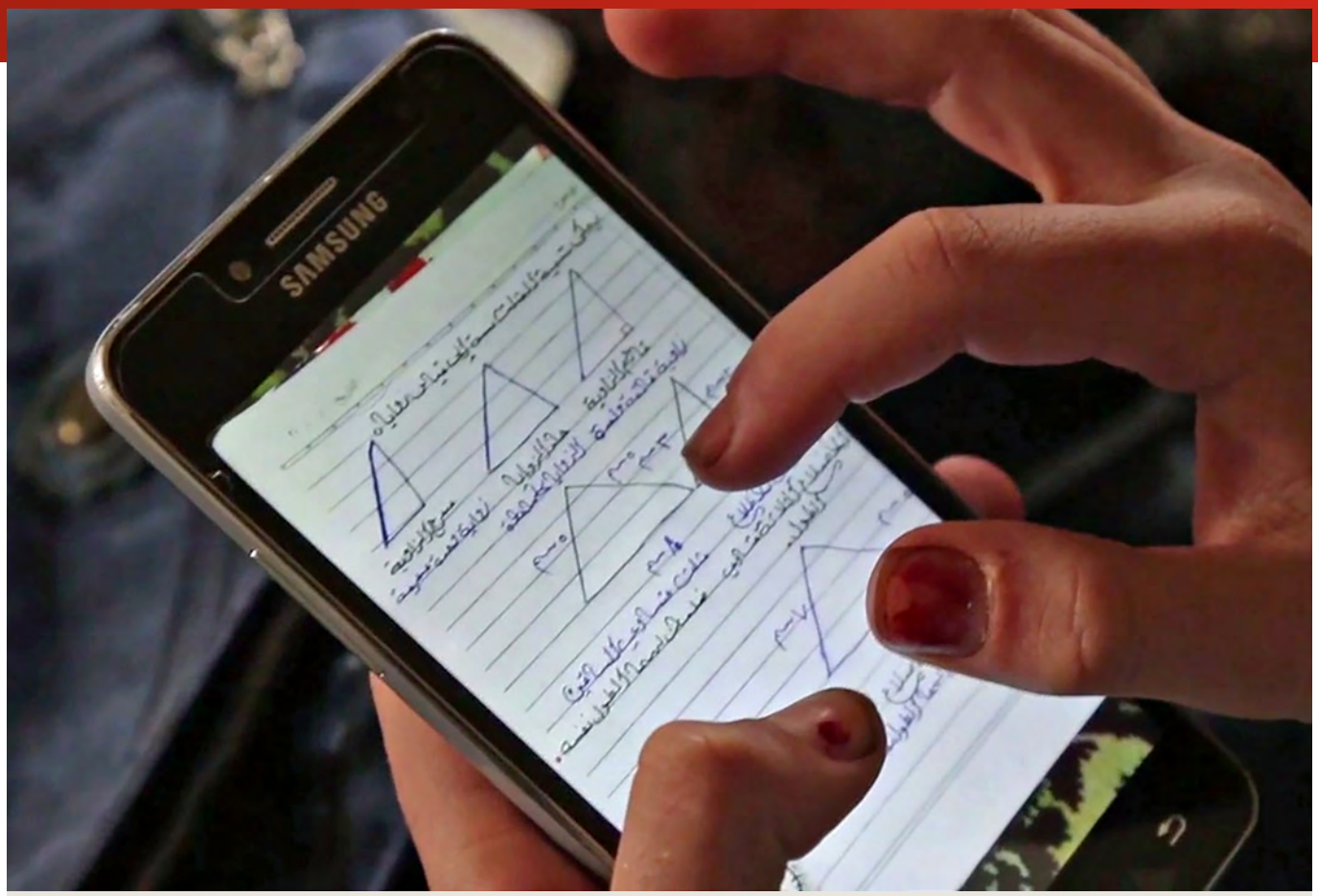
Develop practical and consistent data management systems and processes

The sector needs to have practical data protection and management guidelines that are more contextually and operationally relevant. This includes determining a relevant approach to true, active, and informed consent for data capture, and the processing and sharing of children's personal, sensitive and/or group data, particularly during innovation or experimentation processes.

Agencies also need to invest in better alignment of systems for data storage and security so that country offices are not managing multiple systems, depending on member office resources and preferences.

Staff also call for additional support and guidance on data sharing with partners, re-use of community mobile phone numbers for secondary purposes during an emergency, use of WhatsApp for child protection case management in camp settings, setting up encryption on open source data collection applications, data ownership, data retention and deletion.

In order to implement these recommendations, Save the Children should convene a cross-organisational working group to create and resource a roadmap for the organisation. Localised and ongoing research is also required on how migrating and displaced children are accessing and using online platforms and services in order to stay up to date on the risks and potential harms that need attention. A co-ordinated and joined up sector wide approach is crucial to delivering against these recommendations.



Save the Children's partner Syria Relief

Useful guidance and toolkits

- DIAL: Principles for Digital Development[181] (additional guidance is forthcoming on inclusion)
- Girl Effect: Digital Safeguarding Tips and Guidance[182] (see chapter on Safe Research)
- Response Innovation Lab[183] (Save the Children is a partner)
- HIF and Erlha: Humanitarian Innovation Guide[184] (practical ethics guidance is forthcoming)
- Do no harm: A taxonomy of the challenges of humanitarian innovation[185]
- UK Children's Commissioner: Who Knows What about Me[186]
- London School of Economics: My Privacy UK[187]
- Girl Effect: Digital Safeguarding Tips and Guidance[188]
- End Violence against Children: Online resources on child online safety during COVID-19[189]
- Plan International: Safeguarding Children and Young People Policy Guidance: Safety on Online Platforms[190]
- Save the Children: Existing guidelines on child online safety
- Save the Children: Safeguarding & Digital Technology for Programs Tipsheet: Digital & Social Media platforms
- UNICEF: Responsible data for children (RD4C)[191]
- UNICEF: Faces Fingerprints and Feed (Guidance on biometrics)[192]
- UNOCHA: Data Responsibility Guidelines[193]
- UN: Principles on Personal Data Protection[194]
- USAID: Considerations for Responsible Data[195]

ANNEXES

Annex 1
Initial risk assessment

The questions below can serve as an initial risk assessment support tool to explore and identify potential for harm.

1	Designing and implementing with inclusion in mind
Big picture question: **What is the risk of excluding migrating and displaced children when we introduce innovations, digital programming or data initiatives?**	What do we know about the children we want to engage or support in terms of their literacy, language, culture, traditions, migration or displacement status, past experiences or trauma, ethnicity, levels of stress or threat, gender identity and how gender is expressed in their culture/country of origin and other countries they may be passing through or residing in? Are we excluding these children due to their general circumstances, context or identity?
	Are we excluding children because they don't have access to or use of digital devices or the internet? What do we know about how migrating and displaced children access the internet or digital devices? Do they own devices? What kinds of devices? Or do they borrow them or share them? From whom? How often? Does anyone else control or review how they use the device? What social media or other sites or channels do they use? What are their experiences of harassment or exclusion in the past?
	Are we designing data approaches that reinforce bias, oppression and injustice? How can we ensure that our data analytics don't replicate bias or serve to exclude how we collect/access/use interpret and analyse data, including algorithms that are missing people, biased, contribute to oppression or injustice or other harms, or specific decisions that harm/leave out certain children or groups of children?
	Are children self-excluding out of fear or lack of trust? Have we considered the possibility that children don't want to be counted/tracked because of privacy concerns? Or that they might not want to participate due to past experiences of being harassed, bullied, or otherwise harmed? Have we considered that their fears might be valid and found alternative ways for them to participate or to be counted and heard?

2	Introducing digital programming and innovations
Big picture question: **Are we introducing responsible digital programming and innovations?**	Is this a real problem for the people we are creating or designing programmes for? Who have we asked? What did they tell us?
	What is our motivation for doing this? What expressed need, right, or problem are we responding to? What research/evidence do we have about the nature of what is needed and how it might be designed?
	Has this or something like it been done before? What have we learned and applied from past experiences?
	Is this problem 'ours' to address, or are others better placed to address it? Are local actors already doing something that we could support? How will local actors be engaged now and later?
	Is this problem one that can be solved by technology, information or communication, or more/different data? Are there other ways this problem could be solved? Why is a technology or data innovation the best approach? How will it be integrated into the wider programme or ecosystem? What people, processes and political will are needed to accompany the technology?
	Do the benefits for migrating and displaced children and their communities outweigh the risks and potential for harm? How have we assessed this and who was involved? What unintended consequences or negative outcomes might there be and for whom?
	Is there sufficient training, technical literacy, and guidance in place?
	What will happen when our funding or our project ends and the product or service is no longer available? What will happen to the data that we collected?
	Who might have a malicious intent or interest in this initiative or the data we would collect? How can we reduce the threats?
	How will the project or the data be governed and how will we manage transparency and accountability to children? What laws and regulations do we need to follow?

3	**Using digital communications or encouraging children to participate in the digital environment**
Big picture question: **What risks or potential harms are we introducing or exacerbating by exposing migrating or displaced children to the digital environment?**	When children use the internet and mobile phones on their own, are we exposing them to risk through contact, content or conduct? Are we exposing them to privacy violations, stigma or potential reputational risk? Have we found ways to help children navigate these risks? Do they know where to get help or support?
	When Save the Children introduces devices or digital channels to children, have we designed platforms and participation in ways that reduce risk, such as providing healthy online communities with sufficient moderation?
	When Save the Children uses digital platforms or social media channels in its programming, advocacy and communications work, have we worked with children and their families to help them understand where and how their photos and words will be used and what the risks could be? Are we anonymising them sufficiently? Have we provided channels they can use to revoke their consent and signposted them to where they can find support if they suffer any type of harm?
	When we and our partners encourage children to engage online, have we put controls in place to protect children?
	When we are working with children who have their own devices and social media profiles, are we finding ways to help them protect themselves from harmful content and contact?
	Are we aware of and following legal regulations and industry standards related to children's access to online platforms?

4	Capturing, processing and/or sharing children's data
Big picture question: **What risks or potential harms are we introducing or exacerbating by capturing, processing or sharing children's data?**	Are we following our data security protocols and data protection policies? Have we consulted with our IT colleagues before introducing any new tools, apps, platforms or data initiatives?
	Have we adapted any Save the Children policies to the local context, and taken into account local data privacy regulations?
	Have we planned how we will secure and protect data throughout the data lifecycle? Are we using new or emerging data approaches that require a more detailed assessment to ensure they are not putting children at risk of harm?
	Have we vetted any data partners for their capacity to protect children's data?
	Have we ensured lawful bases for data collection and processing, including consent or other procedures? Have we ensured we are collecting and processing only the data we need?
	Have we addressed programmatic implications due to unequal power dynamics, lack of transparency and accountability, and loss of trust when data is shared with government or the private sector?
	Have we put in place data governance, transparency and accountability to beneficiaries?
	Have we conducted a risk-benefit assessment before engaging in a data collection or processing exercise?

Annex 2
Relevant sector policies, guidelines and resources

Organisation	Theme(s)	Document	Summary of document & link
Response Innovation Lab	Innovation Digital Humanitarian	Evidencing Innovation Toolkit	The toolkit aims to help organisations better use monitoring, evaluation, research and feedback to develop prototypes, pilot them, and evaluate and learn from the process. https://responseinnovationlab.com/evidencing-innovation/
Digital Impact Alliance	Digital	Principles for Digital Development	Principles for Digital Development is a living document that lays out nine principles to help organisations design impactful and sustainable digital programmes and initiatives. https://digitalprinciples.org/
Save the Children	Online safety	Keeping Children Safe Online: a guide for organisations	The guide was developed for international NGOs that use social media with children and young people, particularly those working in developing countries where there is an increasing use of social media and growing need to protect children online. https://resourcecentre.savethechildren.net/node/8563/pdf/kcs_online_guidance_2014.pdf
ITU and UNICEF	Online safety	Guidelines on Child Online Protection	Children: https://resourcecentre.savethechildren.net/node/8473/pdf/gl-child-2009-e.pdf Parents, guardians and educators: https://resourcecentre.savethechildren.net/node/8472/pdf/guidelines-educ-e.pdf Industry: https://resourcecentre.savethechildren.net/node/8470/pdf/bd_broch_industry0809.pdf Policy makers: https://resourcecentre.savethechildren.net/node/8471/pdf/guidelines-policy_makers-e.pdf
Save the Children	Online safety	Operational Handbook for Child Online Safety Centres	This handbook presents good practice examples of Safer Internet Centres and analysis of their work. It contains information, suggestions and guidelines with recommendations for a range of ideas that could be implemented in Serbia to improve the protection of children on the internet. https://resourcecentre.savethechildren.net/node/15493/pdf/operational_handbook_for_child_online_safety_centres.pdf
End Violence Against Children	Online safety COVID-19	Online resources on child online safety during COVID-19	The End Violence Against Children campaign compiled different resources for keeping children safe online during the move to virtual and remote services as a result of the COVID-19 pandemic. https://www.end-violence.org/safe-online#covid-19

Organisation	Theme(s)	Document	Summary of document & link
Europol	Online safety COVID-19	COVID-19: Sexual Exploitation	Europol created an online set of tips for parents and educators on how to keep children safe online during the COVID-19 pandemic and prevent child sexual exploitation. https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation
World Vision	Children Digital Humanitarian	Partnership Policy on Global Data Protection and Privacy (2019)	This policy provides an overarching framework for global data protection and privacy at World Vision, documenting the data protection and privacy principles and policies required to ensure there is consistency in data protection and privacy, compliance with applicable laws, good practice, protection of personally identifiable information (PII), and minimisation of the risks of regulatory compliance failure and reputational damage. It is the primary policy under which all other data protection and privacy related policies reside. Not online, but referred to in this discussion paper: https://www.wvi.org/sites/default/files/Discussion%20Paper%20-%20Data%20Protection%20Privacy%20%26%20Security%20for%20Humanitarian%20%20%26%20Development%20Programs%20-%20FINAL.pdf
UNICEF and ICRC	Children Digital Humanitarian	Ethical considerations when using geospatial technologies for evidence generation (2018)	Geospatial technologies have transformed the way we visualise and understand social phenomena and physical environments. There are significant advantages in using these technologies and data however, their use also presents ethical dilemmas such as privacy and security concerns as well as the potential for stigma and discrimination resulting from being associated with particular locations. Therefore, the use of geospatial technologies and resulting data needs to be critically assessed through an ethical lens prior to implementation of programmes, analyses or partnerships. This paper examines the benefits, risks and ethical considerations when undertaking evidence generation using geospatial technologies. It is supplemented by a checklist that may be used as a practical tool to support reflection on the ethical use of geospatial technologies. https://www.unicef-irc.org/publications/971-ethical-considerations-when-using-geospatial-technologies-for-evidence-generation.html
UNICEF	Children Digital Humanitarian	Faces, Fingerprints and Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes (2019)	This document outlines the 10 key questions and criteria that UNICEF programmes are encouraged to ask when evaluating whether to invest or support the use of biometric technologies as part of their programming. These questions provide a critical lens to help weigh the benefits and risks and ensure that appropriate management strategies are in place so that biometrics can be used safely. https://data.unicef.org/resources/biometrics/

Organisation	Theme(s)	Document	Summary of document & link
PIM (coalition of various actors)	Children Digital Humanitarian	Protection Information Management (PIM) Training Resource Pack (2018)	Protection Information Management (PIM) refers to the principled, systematised and collaborative processes to collect, process, analyse, store, share, and use data and information to enable evidence-informed action for quality protection outcomes. These five training modules aim to help protection staff learn to manage data responsibly. http://pim.guide/uncategorized/pim-training-resource-pack/
Stanford	Children Digital Trafficking	Getting to Good Human Trafficking Data: Everyday Guidelines for Frontline Practitioners (2018)	This document serves as a catalyst to assess and enhance existing data collection efforts – tailored to the local context and with a view to the regional potential – for good, responsible data to combat human trafficking. This guide is intended to serve as a reference document, offering baseline standards and recommendations based on current understanding (at the time of publication) of good, responsible data practices. https://handacenter.stanford.edu/publications/getting-good-human-trafficking-data-everyday-guidelines-frontline-practitioners
UNICEF	Children Digital	Responsible Data for Children (2019)	RD4C seeks to build awareness of the need for special attention to data issues affecting children, especially in this age of changing technology and data linkage. It encourages governments, communities, and development actors to put the best interests of children and a child rights approach at the centre of data activities. Drawing upon field-based research and established good practice, RD4C aims to highlight and support best practice data responsibility; identify challenges and develop practical tools to assist practitioners in evaluating and addressing them; and encourage a broader discussion on actionable principles, insights, and approaches for responsible data management. https://rd4c.org/
Girl Effect	Children Digital	Digital Safeguarding Tips and Guidance (2018)	The document offers staff and partners guidance on how to protect the privacy, security and safety of adolescent girls when developing digital tools and platforms, partnering with others, or using data in monitoring, evaluation and learning efforts. The 2018 version has been updated to include GDPR. https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf

Organisation	Theme(s)	Document	Summary of document & link
Children's Commissioner for England	Children Digital	Who Knows What About Me (2018)	The Children's Commissioner is concerned that information collected about a child today might jeopardise their future, potentially affecting whether they are offered a university place, job or financial products such as insurance or credit. This online report maps out the specific ways that children's data is being harvested in the UK and explores the possible implications of this. https://www.childrenscommissioner.gov.uk/our-work/digital/who-knows-what-about-me/
London School of Economics	Children Digital	My Privacy UK (2019)	A data and privacy toolkit aimed at children in the UK. Covers data, rights, surveillance and tracking, unintended consequences of online data tracking, how to protect your privacy, and how to get help. http://www.lse.ac.uk/my-privacy-uk
EU	Children Digital	General Data Protection Regulation (2018)	The General Data Protection Regulation (GDPR) places conditions on processing any kind of personal data. It includes specific policies for the protection of children's rights, requiring that children must be able to understand privacy notices and that online services offered for children may only process data with a guardian's consent unless they are preventative or counselling services. Individual rights according to the GDPR include: 1 the right to be informed; 2 the right of access; 3 the right to rectification; 4 the right to erasure; 5 the right to restrict processing; 6 the right to data portability; 7 the right to object; 8 rights in relation to automated decision making and profiling. https://gdpr.eu/
COPPA	Children Digital	Children's Online Privacy and Protection Act (2000)	The primary goal of COPPA is to give parents control over what information is collected from their young children online. The act was designed to protect children under age 13 while accounting for the dynamic nature of the internet, and applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children. COPPA also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13, or directly from users of another website or online service directed to children. https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions

Organisation	Theme(s)	Document	Summary of document & link
UN OCHA Centre for Humanitarian Data	Digital Humanitarian	Data Responsibility Guidelines (2019)	The OCHA Data Responsibility Guidelines offer a set of principles, processes and tools that support the safe, ethical and effective management of data in humanitarian responses. The core audience for the guidelines is OCHA staff involved in managing humanitarian data across OCHA's core functions of coordination, advocacy, policy, humanitarian financing and information management, with a primary focus on the field. https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf
UN System	Digital Humanitarian	Principles on Personal Data Protection (2019)	These principles set out a basic framework for the processing of "personal data", which is defined as information relating to an identified or identifiable natural person ("data subject") by, or on behalf of, the United Nations System Organisations in carrying out their mandated activities. The principles aim to: i) harmonise standards for the protection of personal data across the United Nations System Organisations; ii) facilitate the accountable processing of personal data for the purposes of implementing the mandates of the United Nations System Organisations; and iii) ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy. https://www.unsystem.org/principles-personal-data-protection-and-privacy
UNDG	Digital Humanitarian	UNDG Big Data Guidance note (2017)	Sets out general guidance on data privacy, data protection and data ethics concerning the use of big data, collected in real time by private sector entities as part of their business operations, and shared with the UN for the purposes of strengthening operational implementation of programmes to support the achievement of the 2030 Agenda for Sustainable Development. The guidance note is designed to: establish common principles; serve as a risk-management tool taking into account fundamental human rights; and set principles for obtaining, retaining, using and ensuring quality control of data from the private sector. https://undg.org/wp-content/uploads/2017/03/UNDG-Big-Data-Guidance-Note.pdf
World Food Programme	Digital Humanitarian	Guide to Personal Data Protection and Privacy (2016)	A comprehensive data protection guide from the WFP. https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

Organisation	Theme(s)	Document	Summary of document & link
International Organisation of Migration and Harvard Humanitarian Initiative	Digital Humanitarian	Signal Code (2017)	The Signal Code aims to help advance current and future efforts to create shared ethical obligations for practitioners. The primary goal of the code is to help reduce and prevent the threat of harm to vulnerable populations negatively affected by humanitarian information activities that may violate their rights. https://signalcode.org/
Oxfam	Digital Humanitarian	Responsible Data Policy (2016)	A policy that focuses on Oxfam's commitment to treat programme data with respect and uphold the rights of those whom the data relates to. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/575950/ml-oxfam-responsible-program-data-policy-en-270815.pdf;jsessionid=9D9400BB916458CB419CE081D832B2B3?sequence=1
GSMA	Digital Humanitarian	Guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak (2014)	When Call Data Records (CDRs) were used to help in the response to the Ebola outbreak, mobile operators wished to ensure that mobile users' privacy was respected and protected and any associated risks were addressed. This document outlines, in broad terms, the privacy standards that mobile operators would apply when subscriber mobile phone data was used for responses to the Ebola outbreak. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/GSMA-Guidelines-on-protecting-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-Ebola-outbreak-_October-2014.pdf
Sunlight Foundation	Digital Migrants	Protecting data, protecting residents (2017)	Ten principles for municipal authorities on managing data. This document was created as a way to help municipalities protect migrants and undocumented persons in the US following the 2016 Presidential election. https://sunlightfoundation.com/wp-content/uploads/2017/02/Protecting-data-protecting-residents-whitepaper.pdf
USAID	Digital Humanitarian	Considerations for Responsible Data (2019)	This document aims to provide USAID staff and local partners with a framework for identifying and understanding risks associated with development data. It highlights important concerns and provides actionable advice to help those who use data in development programmes to maximise utility while also managing risk. A literature review is also included, as well as a legal review that looks at which US privacy laws do and do not cover non-citizens including undocumented migrants. https://www.usaid.gov/sites/default/files/documents/15396/USAID-Using DataResponsibly.pdf

Organisation	Theme(s)	Document	Summary of document & link
ICRC	Digital Humanitarian	Data Protection in Humanitarian Action (2017)	This publication builds on previous guidance from the ICRC and includes new guidance on the management of personal data in humanitarian situations, including guidance on data analytics and big data; use of UAVs, drones and satellite imagery; remote sensing; biometrics; cash transfer programming; cloud services and mobile messaging apps. http://reliefweb.int/sites/reliefweb.int/files/resources/4305_002_Data_protection_and_humanitarian_action.pdf
ICRC	Digital Humanitarian	Biometrics Policy (2019)	As new technology provides new opportunities to use biometrics in different contexts, the ICRC has adopted a dedicated Biometrics Policy to facilitate their responsible use and address the data protection challenges this poses. https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf
CARE	Digital Humanitarian	Responsible Data Maturity Model (2019)	An open source tool developed for CARE to help point persons in organisations or teams to improve data practices and data ethics. The model can be adapted and used in ways that are appropriate for other team members who do not have responsible data as their main, day-to-day focus. https://lindaraftree.com/2019/10/17/a-responsible-data-maturity-model-for-non-profits/
Mercy Corps	Digital Humanitarian	Guidance on Weaponization of Information (2019)	This assessment explores how social media can contribute to offline conflict by examining real-world case studies. The paper provides a framework for response. https://www.mercycorps.org/sites/default/files/Weaponization_Social_Media_FINAL_Nov2019.pdf

Annex 3
Consultations carried out

Consultations within Save the Children	
Team or region	**Number**
Operations and programming teams	13
Lebanon	10
Ethiopia	5
El Salvador	7
Afghanistan	3
The Balkans	9

Consultations with external organisations and experts	
Organisation & expert areas	**Number**
UNHCR: child protection, accountability	2
The Engine Room: biometrics and digital ID	1
OCHA: Centre for Humanitarian Data	1
GovLab: responsible data for children	1
Yale: humanitarian data and ethics	1
UNICEF: data, safeguarding, research ethics	2
ChildFund: violence against children online	1
World Vision: innovation, humanitarian data	1
InterAction: data, protection	2

Endnotes

1
UNHCR, 2020.
'Global Trends Report: Forced Displacement in 2019.' https://www.unhcr.org/5ee200e37.pdf

2
Campo, S., and Raymond, N., 2019.
'Displaced Children and Emerging Technologies: Save the Children's opportunities for investment and impact', Save the Children. https://resourcecentre.savethechildren.net/node/15382/pdf/stc_tech_innovation_study_v7_digital.pdf

3
UNHCR, 2020.
'Global Trends Report: Forced Displacement in 2019.' https://www.unhcr.org/5ee200e37.pdf

4
Campo and Raymond, op. cit.

5
Ibid.

6
Ibid.

7
Raftree, L., 2020.
'Remote Monitoring in the Time of Coronavirus.' http://merltech.org/remote-monitoring-in-the-time-of-coronavirus/

8
A Chatham House rule gathering on 'Digital Dignity' hosted by the IFRC at Wilton Park, UK, in October 2019 debated this issue among others.

9
Ibid.

10
Parker, B., 2020.
'Aid policy trends to watch in 2020.' https://www.thenewhumanitarian.org/feature/2020/1/2/Humanitarian-aid-policy-reform

11
The Grand Bargain commits donors and aid organisations to providing 25 per cent of global humanitarian funding to local and national responders by 2020, along with additional non-earmarked money, and increased multi-year funding to ensure greater predictability and continuity in humanitarian response, among other commitments.

12
UNICEF, 2017.
'State of the World's Children: Children in the Digital Age.' https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

13
ITU World Telecommunication/
ICT Indicators database, accessed Dec 29, 2019
https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

14
UNICEF, 2017. op. cit.

15
Rowntree, O., 2018.
'The Mobile Gender Gap Report', GSMA: London. https://www.gsma.com/ mobilefordevelopment/wp-content/uploads/2018/04/GSMA_ The_Mobile_Gender_Gap_Report_2018_32pp_WEBv7.pdf

16
UNICEF, 2019.
'Faces, Fingerprints and Feet.'
https://data.unicef.org/resources/biometrics/

17
Ibid.

18
Girl Effect and Vodafone, 2019.
'Real Girls, Real Lives, Connected'.
https://static1.squarespace.com/static/5b8d51837c9327d89d936a30/t/5beaa1700e2e72ed39d21c5b/1542103477055/GE_VO_Full_Report_Digital.pdf

19
Ibid.

20
GSMA, 2019.
'Bridging the Mobile Disability Gap in Refugee Settings'. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/09/M4H_DisabilityGap.pdf

21
Girl Effect and 2CV, (2014–2018).
Series of unpublished research initiatives in India, Indonesia, Bangladesh, Ethiopia, Nigeria, South Africa, and The Philippines.

22
Girl Effect and Vodafone, op. cit.

23
Girl Effect and 2CV, (2014–2018), op. cit.

24
Key informant interview, UN Agency, March 2020.

25
Girl Effect, 2019.
Qualitative Research in Indonesia, unpublished.

26
Raftree, L., 2013.
'Modern Mobility: The role of ICTs in child and youth migration.' Plan International and the Oak Foundation. https://resourcecentre.savethechildren.net/sites/default/files/documents/modern_mobility.pdf

27
Campo and Raymond, op. cit.

28
Humanitarian Innovation Fund and Elrha, 2019.
'Humanitarian Innovation Guide.'
https://higuide.elrha.org/enabling-factors/manage-risk/

29
The Lancet and Financial Times Commission, 2020.
'Governing health futures 2030: growing up in a digital world.' Webinar on Enabling Digital Health Futures in Humanitarian Settings: Session 3 (Sustaining the humanitarian principles in a digital era).

30
Krishnaraj, G., Hunt, M., and Schwartz, L., 2019.
'Asking the important questions of ethical humanitarian innovation'. Elrha. https://medium.com/elrha/asking-the-important-questions-of-ethical-humanitarian-innovation-1189b8c169f0

31
Bergtora Sandvik, K., Lindskov Jacobsen, K., and McDonald, S., 2017.
'Do no harm: A taxonomy of the challenges of humanitarian experimentation'.
https://international-review.icrc.org/sites/default/files/irrc_99_17.pdf

32
Bergtora Sandvik, K., 2016.
'Insecurity in the Humanitarian Cyberspace: A Call for Innovation'. https://www.alnap.org/blogs/insecurity-in-the-humanitarian-cyberspace-a-call-for-innovation

33
Raftree, 2013, op. cit.

34
UNICEF, 2017, op. cit.

35
Aynsley, C., 2014.
'Keeping Children Safe Online: A guide for organisations.' https://resourcecentre.savethechildren.net/node/8563/pdf/kcs_online_guidance_2014.pdf

36
Miller, C., 2018.
'Does Social Media Cause Depression?'
https://childmind.org/article/is-social-media-use-causing-depression/

37
Kidron, Baroness, Evans, A., Afia, J., 2019.
'Disrupted Childhood. The Cost of Persuasive Design'. 5Rights. https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf

38
United Nations Broadband Commission, 2015.
'Combatting Online Violence Against Women & Girls: A Worldwide Wake-Up Call'.
https://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release

39
Blumenfeld, W. and Cooper, R., 2010.
'LGBT and allied youth responses to cyberbullying: Policy implications'.
International Journal of Critical Pedagogy.
http://libjournal.uncg.edu/index.php/ijcp/article/viewFile/72/57

40
Hinduja, S., and Patchin, J., 2010.
'Cyberbullying Research Summary: Cyberbullying and Suicide.'
https://cyberbullying.org/cyberbullying_and_suicide_research_fact_sheet.pdf

41
UNICEF, 2017, op. cit.

42
United Nations Broadband Commission, 2015, op.cit.

43
Blumenfeld and Cooper, 2010, op. cit.

44
Hinduja and Patchin, 2010, op. cit.

45
Bixby, S., 2018.
'LGBT Migrants Fled Persecution Back Home. Then They Fled the Caravan.' https://www.thedailybeast.com/lgbt-migrants-fled-persecution-back-home-then-they-fled-the-caravan

46
Caravita, S., et al., 2019.
'Being Immigrant as a Risk Factor to Being Bullied: An Italian study on individual characteristics and group processes', Child Abuse and Neglect. https://onlinelibrary.wiley.com/doi/10.1111/sjop.12565

47
UNICEF, 2017, op. cit.

48
Human Rights Council, September 17, 2018.
'Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar.' https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf

49
Interview with Save the Children staff in The Balkans, April 2020.

50
Interview with Save the Children staff in El Salvador, April 2020.

51
Bueno, O., 2019.
'"'No Mother Wants Her Child to Migrate:' Vulnerability of Children on the Move in the Horn of Africa." UNICEF Office of Research (Innocenti). https://www.unicef-irc.org/publications/pdf/Child-Migration-Horn-of-Africa-part-1.pdf

52
Dekker, R., Engbersen, G., Klaver, J., and Vonk, H., 2018.
'Smart Refugees: How Syrian Asylum Migrants Use Social Media Information in Migration Decision-Making'. Sage. https://journals.sagepub.com/doi/10.1177/2056305118764439

53
Toaldo, M., 2015.
'Migrations through and from Libya: a Mediterranean challenge.' Istituto Affari Internazionali.

54
United Nations High Commissioner for Refugees, April 2017.
'From a refugee perspective: Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016.'

55
UNODC, 2018.
'Global Study on Smuggling of Migrants'. https://www.unodc.org/documents/data-and-analysis/glosom/GLOSOM_2018_web_small.pdf

56
Interview with Save the Children staff in Switzerland, March 2020.

57
University of Toledo, October 8, 2018.
'Study details link between social media and sex trafficking.' https://phys.org/news/2018-10-link-social-media-sex-trafficking.html

58
Hussain, S., 2019.
'When bills pile up, young people turn to strangers on Venmo.' https://www.latimes.com/business/la-fi-venmo-cash-app-twitter-crowdfund-money-20190602-story.html

59
Privacy International, 2019.
'Experts object to US Immigration & Customs Enforcement's "Extreme Vetting Initiative" that will rely on AI'. https://www.privacyinternational.org/examples/3076/experts-object-us-immigration-customs-enforcements-extreme-vetting-initiative-will.

60
Rivlin-Nadler, M., 2019.
'How ICE Uses Social Media to Surveil and Arrest Immigrants.' The Intercept. https://theintercept.com/2019/12/22/ice-social-media-surveillance/

61
Rafiq, H., and Malak, N., 2018.
'Refuge, Pathways of Youth Fleeing Extremism.' https://www.quilliaminternational.com/wp-content/uploads/2017/02/refuge-pathways-of-youth-fleeing-extremism-executive-summary.pdf

62
Guay, J., Gray, S., Rhynard-Geil, M., Inks, L., 2019.
'The Weaponization of Social Media: How social media can spark violence and what can be done about it'. Mercy Corps. https://www.mercycorps.org/sites/default/files/Weaponization_Social_Media_FINAL_Nov2019.pdf

63
Interviews with staff members from Save the Children office in El Salvador, April 2020.

64
Gelb, A., and Clark, J., 'Identification for Development: The Biometrics Revolution', CGD Working Paper 315, Center for Global Development, Washington, D.C., January 2013.

65
Buolamwini, J., and Gebru, T., 2018.
'Gender Shades: Intersectional accuracy disparities in commercial gender classification', Proceedings of Machine Learning Research, vol. 81, pp. 77–91.

66
UNICEF, 2017. op. cit.

67
Interview with Save the Children staff in El Salvador, April 2020.

68
McDonald, S., 2016.
'Ebola: A Big Data Disaster'. https://cis-india.org/papers/ebola-a-big-data-disaster

69
UNICEF Office of Research-Innocenti, 2020.
'Digital Contact Tracing and Suveillance during COVID-19'. https://www.unicef-irc.org/publications/1096-digital-contact-tracing-surveillance-covid-19-response-child-specific-issues-iwp.html

70
Zittrain, J., 2020.
'Is Digital Contact Tracing over Before it Began?' https://medium.com/berkman-klein-center/is-digital-contact-tracing-over-before-it-began-925c72036ee7

71
ICRC, 2019.
'The Humanitarian Metadata Problem: Doing No Harm in the Digital Era'. https://blogs.icrc.org/inspired/2019/06/01/footprints-ether-metadata/?linkId=100000009668523

72
Young, A., (forthcoming).
'Responsible Group Data for Children'. UNICEF.

73
Arbuckle, L., April 27, 2020.
'Aggregated data provides a false sense of security.' https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/

74
Hosein, G., and Nyst, C., 2013.
'Aiding Surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries'. Privacy International. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229

75
Key informant interview, external source, February 2020.

76
Privacy International, 2019.
'Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers.' https://www.privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

77
Privacy International, 2019.
'Who supplies the data, analysis, and tech infrastructure to US immigration authorities?' https://www.privacyinternational.org/feature/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities

78
Privacy International, 2011, op. cit.

79
ICRC, 2019.
'Digital Dignity in armed conflict: a roadmap for principled humanitarian action in the age of digital transformation'. Shared at a 'Digital Dignity' convening hosted by the IFRC at Wilton Park, UK in October 2019. The convening was managed under Chatham House Rule, therefore identifying information from this case has not been included here.

80
Ibid.

81
Internews, 2011.
'Lost: Syrian Refugees and the Information Gap'. https://www.internews.org/resource/lost-syrian-refugees-and-information-gap

82
Latonero, M., Poole, D., Berens, J., 2018.
'Refugee Connectivity: A survey of mobile phones, mental health, and privacy at a Syrian refugee camp in Greece.' Harvard Humanitarian Initiative and Data & Society.
https://datasociety.net/wp-content/uploads/2018/04/Refugee_Connectivity_Web.MB4_.8-2.pdf

83
Note: This type of information doesn't seem to be available specifically for children

84
Casarosa, F., 'Protection of minors online: available regulatory approaches', Journal of Internet Law, vol. 9, March 2011, pp. 25–35.

85
Kaurin, D., 2019.
'Data Protection and Digital Agency for Refugees.' World Refugee Council Research Paper No 12. https://www.cigionline.org/sites/default/files/documents/WRC%20Research%20Paper%20no.12.pdf

86
Hayes, Ben and Massimo Marelli, 2019.
'Facilitating innovation, ensuring protection: the ICRC Biometrics Policy'. ICRC Humanitarian Law & Policy. https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/

87
Montoya-Galvez, C., 2020.
'U.S. collecting DNA samples from some migrants — including teens — in first stage of program'. https://www.cbsnews.com/news/us-collecting-dna-samples-from-migrants-including-children-first-stage-of-program/

88
Privacy International, 2011, op. cit.

89
Boyd, D., and Crawford, K., 2012.
'Critical Questions for Big Data,' Information, Communication and Society, Vol 15 – Issue 5: A decade in Internet time: The dynamics of the Internet and Society. Taylor and Francis Online.
https://www.tandfonline.com/doi/abs/10.1080/1369118X.2012.678878

90
UNCTAD, 2020
'Data Protection and Privacy Legislation Worldwide.'
https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

91
The DLA Piper's Global Data Protection Handbook site provides information on data privacy policies around the world, including whether there are specific policies covering children's data and the country's age of consent for data collection.
https://www.dlapiperdataprotection.com/#handbook/world-map-section

92
Key informant interview, external source, February 2020.

93
European Union, 2017.
'General Data Protection Regulation.'
https://gdpr.eu/

94
US Government's Federal Trade Commission, 2000.
'Children's Online Privacy and Protection Act.'
https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions

95
Privacy International, 2011, op. cit.

96
Green, S., Chandrasekharan, S., Schwegmann, C., Cohen, J., Sullivan, C., Raftree, L., Bari Farahi, A., Getachew, N., 2017.
'Responsible Data Practices: Literature Review.' USAID.

97
UNICEF, 2017. op. cit.

98
Nyst, C., 2017.
'Privacy, protection of personal information and reputation rights,' Children's Rights and Business in a Digital World Discussion Paper Series, United Nations Children's Fund, March 2017.

99
Bajak, Frank, 2018.
'Groups demand end to info-sharing on asylum-seeking children.' AP News.
https://apnews.com/81787a5897704a0cae82a9ceb0eea271

100
See https://resourcecentre.savethechildren.net/

101
Staff preferred to speak off the record in some instances, and in these cases we have not listed their offices or positions.

102
Interviews with Save the Children staff working in the areas of technology and innovations, March 2020.

103
Interviews with Save the Children staff working on innovations, February and March 2020.

104
Interview with Save the Children International staff, February 2020.

105
Interview with Save the Children staff at a Member office, February 2020.

106
Interview with Save the Children country Office Program staff, April 2020.

107
Interview with Save the Children staff in The Balkans, April 2020.

108
Interview with Save the Children staff in The Balkans, February 2020.

109
Ivanović, 2019, op. cit.

110
Interviews with Save the Children staff in Denmark, Switzerland and the United States, January-March 2020.

111
Interview with Save the Children staff in El Salvador, April 2020.

112
Interview with staff from Save the Children The Balkans Country Office Communications staff, April 2020.

113
Interview with staff from Save the Children Country Office Communications staff, April 2020.

114
Interview with Save the Children staff in The Balkans, April 2020.

115
Interviews with Save the Children staff in The Balkans, El Salvador, Lebanon, Ethiopia, Afghanistan, and Save International, April 2020.

116
Interview with Save the Children staff in El Salvador, April 2020.

117
Interviews with Save the Children staff in Lebanon, Ethiopia, El Salvador, and the Center.

118
European Union, op. cit.

119
Interview with Save the Children International staff, February 2020.

120
Interview with Save the Children International staff, February 2020.

121
Interviews with Save the Children staff in The Balkans, April 2020.

122
Interview with Save the Children International staff, February 2020.

123
Interview with Save the Children staff in The Balkans staff, 2020.

124
Interview with Save the Children staff in Afghanistan, El Salvador, The Balkans and Save International, April 2020.

125
Interview with Save the Children staff in El Salvador, April 2020.

126
Interview with Save the Children staff in The Balkans, April 2020.

127
Interviews with Save the Children staff in The Balkans, April 2020.

128
Campo and Raymond, op. cit.

129
Raftree, 2018, op. cit.

130
Raftree, 2018, op.cit.

131
Raftree, 2018, op. cit.

132
Raftree, 2018, op.cit.

133
Young, Andrew; Stuart Campo; Stefaan G. Verhulst. 2019. "Responsible Data for Children: Synthesis Report." https://rd4c.org/images/rd4c-report-final.pdf

134
Key Informant Interview, External Source, February 2020.

135
Key Informant Interview, External Source, February 2020.

136
Response Innovation Lab, Humanitarian Innovation Fund, START Network, Global Alliance for Humanitarian Innovation, Accountability and Learning Project and UKAID, 2018. "Evidencing Innovation Toolkit."

137
Note: Save the Children was involved in testing this Innovation Toolkit.

138
'Principles for Digital Development', living document. https://digitalprinciples.org/

139
Raftree, Linda, 2018. "Digital Safeguarding Tips and Guidance" Girl Effect https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf

140
Bergtora Sandvik, Jacobsen and McDonald, op. cit.

141
Bueti, Cristina, Maria Jose Cantarino de Frias, John Carr, Carstensen, D., 2009. 'Guidelines for Children on Child Online Protection'. https://resourcecentre.savethechildren.net/node/8473/pdf/gl-child-2009-e.pdf

142
International Telecommunication Union and UNICEF, 2014. 'Guidelines for Industry on Child Online Protection'. https://resourcecentre.savethechildren.net/node/8470/pdf/bd_broch_industry0809.pdf

143
International Telecommunication Union and UNICEF, 2014. 'Guidelines for Policy Makers on Child Online Protection'. https://resourcecentre.savethechildren.net/node/8471/pdf/guidelines-policy_makers-e.pdf

144
International Telecommunication Union and UNICEF, 2014. 'Guidelines for Parents, Guardians and Educators on Child Online Protection.' https://resourcecentre.savethechildren.net/node/8472/pdf/guidelines-educ-e.pdf

145
Aynsley, op. cit.

146
Ivanović, 2019, op. cit.

147
End Violence against Children, April 2020. 'Stay Safe at Home. Stay Safe Online.' https://www.end-violence.org/safeonlinecovid

148
Europol, April 2020. 'COVID-19: Child Sexual Exploitation.' https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation

149
Raftree, 2018, op. cit.

150
Lutz, A., Doornbos, A., Kehl, A., Ghee, A., and DePauw, L., 2017. 'Protection, Privacy and Security for Humanitarian & Development Programs.' Edited Sherrie Simms. https://www.wvi.org/sites/default/files/Discussion%20Paper%20-%20Data%20Protection%20Privacy%20%26%20Security%20for%20Humanitarian%20%20%26%20Development%20Programs%20-%20FINAL.pdf

151
UNICEF and ICRC, 2018, "Ethical considerations when using geospatial technologies for evidence generation" https://www.unicef-irc.org/publications/971-ethical-considerations-when-using-geospatial-technologies-for-evidence-generation.html

152
UNICEF, 2019, op. cit.

153
Protection Information Management Coalition, 2018. 'Protection Information Management (PIM) Training Resource Pack'. http://pim.guide/uncategorized/pim-training-resource-pack/

154
Brunner, J., 2018. 'Getting to Good Human Trafficking Data: Everyday Guidelines for Frontline Practitioners.' Stanford. https://humanrights.stanford.edu/publications/getting-good-human-trafficking-data-everyday-guidelines-frontline-practitioners

155
Young, Campo, and Verhulst, op. cit.

156
Raftree, 2018, op. cit.

157
Children's Commissioner for England, 2018. 'Who Knows What About Me?' https://www.childrenscommissioner.gov.uk/our-work/digital/who-knows-what-about-me/

158
London School of Economics, 2019. 'My Privacy UK'. http://www.lse.ac.uk/my-privacy-uk

159
UN OCHA, 2019. 'Data Responsibility Guidelines.' https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf

160
United Nations, 2019. 'Principles on Personal Data Protection'. https://www.unsystem.org/principles-personal-data-protection-and-privacy

161
UNDG, 2017. 'Big Data Guidance Note.' https://undg.org/wp-content/uploads/2017/03/UNDG-Big-Data-Guidance-Note.pdf

162
World Food Programme, 2016. 'Guide to Personal Data Protection and Privacy.' https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

163
Raftree, L., 2019. 'Responsible Data Maturity Model.' CARE https://lindaraftree.com/2019/10/17/a-responsible-data-maturity-model-for-non-profits/

164
Harvard Humanitarian Initiative and Signal Program on Human Security and Technology, 2016. 'The Signal Code.' https://signalcode.org/code-intro/

165
Oxfam, 2016.
'Responsible Data Policy.'
https://oxfamilibrary.openrepository.com/bitstream/handle/10546/575950/ml-oxfam-responsible-program-data-policy-en-270815.pdf;jsessionid=9D9400BB916458CB419CE081D832B2B3?sequence=1

166
GSMA, 2014.
'Guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak.' https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/GSMA-Guidelines-on-protecting-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-Ebola-outbreak-_October-2014.pdf

167
Sunlight Foundation, 2017.
'Protecting Data, Protecting Residents.'
https://sunlightfoundation.com/wp-content/uploads/2017/02/Protecting-data-protecting-residents-whitepaper.pdf

168
Green et al. op. cit.

169
ICRC, 2017.
'Handbook on Data Protection in Humanitarian Action.' http://reliefweb.int/sites/reliefweb.int/files/resources/4305_002_Data_protection_and_humanitarian_action.pdf

170
ICRC, 2019.
'Biometrics Policy.' https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf

171
Guay, Gray, Rhynard-Geil and Inks, op. cit.

172
'Harvard Humanitarian Initiative and Signal Program on Human Security and Technology', 2016, op. cit.

173
Young, Campo, and Verhulst, op. cit.

174
Key informant interview, external source, February 2020.

175
Key informant interview, external source, February 2020.

176
Key informant interview, external source, February 2020

177
Key informant interview, external source, February 2020.

178
Key informant interview, external source, February 2020.

179
UNICEF, Office of Global Insight and Policy, 2020.
'Good Governance of Children's Data'.
https://www.unicef.org/globalinsight/data-governance-children

180
Key informant interview, external source, February 2020.

181
Digital Impact Alliance.
https://digitalprinciples.org/

182
Raftree, 2018, op. cit.

183
Response Innovation Lab.
https://responseinnovationlab.com/evidencing-innovation/

184
Humanitarian Innovation Fund and Elrha, 2019, op. cit.

185
Bergtora Sandvik, Jacobsen and McDonald, op. cit.

186
Children's Commissioner for England, op. cit.

187
London School of Economics, op. cit.

188
Raftree, 2018, op. cit.

189
End Violence against Children, op. cit.

190
Plan International, 2020.
'Global Safeguarding Unit: Guidance on Safeguarding Children and Young People on Online Platforms.' https://plan-international.org/girls-get-equal/how-to-stay-safe-online

191
Young, Campo, and Verhulst, op. cit.

192
UNICEF, 2019, op. cit.

193
UN OCHA, 2019, op. cit.

194
United Nations, op. cit.

195
USAID, op. cit.

Kristiana Marton / Save the Children

Save the Children

Save the Children

Published by

Save the Children International
St Vincent's House
30 Orange Street
London
WC2H 7HH
United Kingdom

+44 (0)20 3272 0300
www.savethechildren.net

First published October 2020