

UNICEF Digital Impact Division white paper

Building Safer Digital Futures

Insights from UNICEF's work in cybersecurity and data governance for child rights

March 2026

© United Nations Children’s Fund (UNICEF), 2026

Design and layout: Green Ink

Cover photo credit: © UNICEF/UNI604705/Josué Diaz

Contents

Executive Summary.....	iii
1. Introduction.....	1
2. Children’s vulnerability in an era of cyber threats.....	2
2.1 The rising threat environment for children’s rights	2
2.2 Why the security of digital systems matters in humanitarian settings.....	2
3. Secure by Design principles for children	4
3.1 Systems design	4
3.2 Operational safeguards.....	5
3.3 Organizational capabilities	6
4. Strengthening governance and accountability for digital systems for children	8
4.1 For government actors.....	8
4.2 For industry actors	8
4.3 For humanitarian and development actors	8
4.4 For all actors	9
5. Conclusion	10
6. References.....	12

Executive Summary

As digital systems play an increasingly important role in children's lives, an important but often neglected question is: **how are children's rights impacted when digital systems lack adequate security and effective governance?** While these issues may be addressed as technical or institutional concerns, their implications for children's safety, dignity and long-term well-being have not been explored consistently.

This white paper captures learnings from UNICEF's Digital Impact Division work in 2025 and early 2026 – particularly through the SafeChild partnership – at the intersection of cybersecurity, data governance and child rights. Drawing on engagements with governments, humanitarian actors, technical institutions and partners, it organizes emerging insights from the practice of protecting child rights when developing and deploying digital systems. In doing so, it introduces **child rights as a distinct and necessary dimension of cybersecurity** that warrants focused attention and sustained dialogue.

Children's data is uniquely sensitive and longlived, yet the systems that collect and process it are often designed without appropriate safeguards.

Cyber incidents affecting education, health, civil registration and humanitarian systems show how security failures can quickly become child rights failures – disrupting access to services, exposing children to harm, or creating risks that may persist throughout their lives. These risks are amplified in low-resource and crisis-affected settings, where governance gaps, capacity constraints and data concentration are most pronounced.

This white paper builds a foundation for future work by identifying core conditions that influence whether digital systems protect or undermine children's rights. It positions **cybersecurity and data governance as foundational enablers of child rights in digital environments**, rather than peripheral considerations.

As digital systems increasingly shape children's lives from birth onwards, addressing cybersecurity and data governance gaps is crucial. Building safer digital futures for children will depend on whether governments, industry and humanitarian actors treat secured and accountable digital foundations as a priority, and invest accordingly.






UNIÓN EUROPEA
Proyecto Estrategia Integral para
Combatir la Desnutrición Crónica

1. Introduction

Children today increasingly rely on digital systems to access essential services such as education, health care, social protection and humanitarian assistance. Digital platforms and technologies are now fundamental to each step of a child's journey through vital services, from enrolling in school to receiving vaccinations, accessing social benefits or seeking support during emergencies.

Yet the digital infrastructure underpinning these systems is increasingly exposed to **cybersecurity threats and uneven data governance practices**. When these systems fail, the consequences for children can be immediate and significant: a compromised database can reveal children's location or identity details, putting their safety, dignity and even survival at risk.

Many digital systems that serve or affect children were never designed with their unique rights or developmental needs in mind. As governments, humanitarian actors and service providers expand the use of digital tools, they **often collect large volumes of data about children** – mostly in low-resource or crisis-affected environments where safeguards are weakest. This creates concentrated datasets that are highly valuable to attackers and particularly harmful when breached.

Cyberattacks targeting health centres, schools, civil registration systems and humanitarian agencies illustrate an emerging trend: **cybersecurity failures can quickly become child rights failures**. When critical systems are disrupted, children can lose access to services such as education, health services or social protection. When personal data is leaked, it can expose children to discrimination, exploitation or retaliation for years, especially in crisis-affected contexts.

In 2025, UNICEF and the Government of Luxembourg created the [SafeChild Partnership](#) to support addressing this urgent challenge. The initiative represents one of UNICEF's first concerted efforts to **support strengthening national cybersecurity ecosystems** and ensuring that the systems children depend on are secured, resilient and rights-respecting by design.

This paper distils UNICEF's initial learnings on how to build **safer and secured digital systems for children**, drawing on engagements with governments, humanitarian partners, technical institutions and academia across a range of contexts through the SafeChild partnership and related initiatives. It explores the conditions that can influence whether digital systems succeed or fail in protecting children's rights – and the governance, architecture and safeguards that can make the difference.

In doing so, it highlights the need for sustained investment in understanding how **cybersecurity and data governance frameworks can be harnessed not only to prevent harm, but to actively enable children's rights** – ensuring that digital tools strengthen, rather than undermine, their protection and participation.

The aim is to position cybersecurity and data governance as foundational tools to protect child rights in the digital age, and to highlight practical, scalable approaches that governments, industry and humanitarian actors can use to embed child-centred protections into digital systems from the outset. By integrating these safeguards early, we can help ensure that digital transformation enhances – rather than endangers – children's rights, safety and wellbeing.

2. Children's vulnerability in an era of cyber threats

2.1 The rising threat environment for children's rights

Children face a range of risks in the digital world, many of which intensify when the digital systems on which they rely lack essential security measures and proper governance. Across multiple engagements, UNICEF has observed that **the long-term risks and impacts of cyber threats for children remain insufficiently understood**. For instance, a child's identity credentials are particularly valuable to identity thieves because misuse can go undetected for years, compounding harm later in life. A breach of health, identity, education or protection-related information can expose a child to targeting, discrimination, exploitation or long-term stigma. Leaked records may follow children for life, limiting access to services and opportunities or putting their safety at risk.

UNICEF's engagements with governments and partners, along with incident analysis, indicate that organizations managing services for children are experiencing an **elevated threat profile due to the aggregation and storage of substantial volumes of sensitive personally identifiable information**, making them attractive targets for cyber adversaries.

In the UK, for example, 60 per cent of secondary schools and 85 per cent of further education colleges (for students aged 16+) [reported a cyberattack](#) or security breach in 2024, and 30 per cent of further and higher education institutions reported **experiencing breaches or attacks at least once a week**.

Partner engagements also indicate that rapid adoption of emerging technologies – including AI-enabled systems – can outpace the development of appropriate governance and security safeguards. Many platforms now collect and process large volumes of behavioural and biometric data – often without adequate transparency – raising the **risk of inappropriate collection, profiling or unintended exposure**. Surveys point to the extent of cyber threats: one [study found](#) 17 per cent of children explicitly referenced hacking, phishing or malware among the threats they experienced (while 72 per cent reported an

online threat of some kind and only 52 per cent said they felt safe online). These figures signal systemic exposure while highlighting that **better evidence is still needed to isolate specific drivers of cyber risk for children** from the broader online risk landscape.

2.2 Why the security of digital systems matters in humanitarian settings

UNICEF's work in fragile and humanitarian settings highlights how these risks are amplified. **In humanitarian and crisis settings, poorly secured digital systems can create direct and immediate threats to children's safety**. Displaced or unaccompanied children are often required to provide personal information in order to access essential services,



© UNICEF/UNI604651/Josué Diaz

yet the environments in which this data is collected and stored may lack even basic protections. When datasets containing location information, family connections or legal status are exposed, they can be misused by hostile actors, putting children and their communities at significant risk.

“

In this digital era, children and youth are being increasingly exploited by means of digital technology and the internet. That is why they are put in unforeseen danger and must be protected.”

– boy, 16, Pakistan
(Our Rights in a Digital World)

A recurring observation is that humanitarian actors **may collect more data than necessary**, particularly in rapid onset or resource-constrained settings. Under pressure to deliver quickly, registration processes sometimes outpace governance, leading to overcollection, long retention periods and the creation of concentrated datasets that become high value targets. Actors should assess whether both the breadth of data collected and the duration of retention are both necessary and proportional.

Real-world cases illustrate the stakes. Biometric devices and data used during conflict have later been seized, raising concerns that sensitive personal data could be repurposed in ways that endanger vulnerable populations, including children. As digital humanitarian services expand, privacy and data protection risks arise in specific domains. Research highlights risk pathways in cash-based transfers, where **digitalization can introduce traceability and profiling concerns if not properly governed**. In education technology (EdTech), one investigation found that 89 per cent of government-endorsed resources compromised privacy protections, indicating significant governance and control gaps around children’s data. In addition, digital networks are increasingly used to identify and lure vulnerable individuals, including children affected by conflict.

UNICEF and partners’ work on strengthening cybersecurity ecosystems also indicates structural challenges that heighten risk: **limited capacity, reliance on external vendors without consistently validated security practices, and operation within weak national cybersecurity and data protection regulatory frameworks**. When systems fail or are compromised, children in these settings face heightened exposure to harm – widening existing inequalities.

3. Secure by Design principles for children

Digital systems that process children's data or mediate their access to essential services should be built on Secure by Design principles, yet UNICEF's engagements suggest that **not all such systems fully incorporate the safeguards required to protect children's unique rights and vulnerabilities**. A rights-respecting security posture begins at the architectural level: understanding what data is collected, how it flows, who can access it and how it is protected across its lifecycle. When these foundations are weak, risks to children can escalate quickly – often more severely and for longer than for adults, given the lasting value of children's data. UNICEF's engagements highlight several design features that can reduce risks to children and children's data.

3.1 Systems design

- **Integrating child-specific assessments** early in system design, including [Cyber Readiness](#), [RD4C](#) and [Digital Child Rights Impact Assessments](#) for agencies

and systems processing children's data. Early assessments prevent costly redesign later.

- **Minimizing data collection and retention** for children, ensuring systems collect only what is strictly necessary for a defined purpose. Overcollection increases the likelihood and severity of harm if compromised.
- **Mapping and governing data flows** across all systems processing children's data, with clear accountability for each stage of the lifecycle. Undocumented data flows often hide unmonitored transfers or risky interconnections.
- **Establishing strong access controls**, authentication mechanisms and Data Loss Prevention measures tailored to children's heightened sensitivity.
- **Involving children in the design** of safety features and policies for digital systems. Children should be engaged in decisions about their digital safety, with their participation adapted to their level of understanding and maturity.

Key initiative

SafeChild: Strengthening national cybersecurity ecosystems for children

The SafeChild Partnership – led by UNICEF with support from the Government of Luxembourg – aims to strengthen the institutional and technical cybersecurity capacity of governments to protect children's rights in the digital age. Recognizing that **systems underpinning child rights are increasingly vulnerable to cyber threats**, UNICEF works with national authorities to embed child-focused principles into cybersecurity strategies, policies and operational practices.

A core element of this effort is the [Cyber Readiness Assessment Toolkit](#), which adapts global frameworks such as the [Inter-American Development Bank's Self-Assessment Tool](#) and the [NIST Cybersecurity Framework](#), integrating UNICEF's child-rights-specific controls. The toolkit allows governments to assess their ability to **govern, identify, protect against, detect, respond to and recover from cyber threats** in the systems that store and process children's data.

SafeChild also invests in capacity-building, cyber-maturity planning and knowledge transfer, helping governments to address policy gaps, strengthen skills and adapt solutions to low-resource settings. In Lesotho, for example, the Toolkit has been piloted to identify vulnerabilities, train staff and test new **cybersecurity measures designed specifically to safeguard children's data**. As emphasized by UNICEF's Representative in Lesotho, Deepak Bhaskaran, "Cybersecurity is a child protection issue. When we secure the systems that serve children, we are safeguarding their futures."

3.2 Operational safeguards

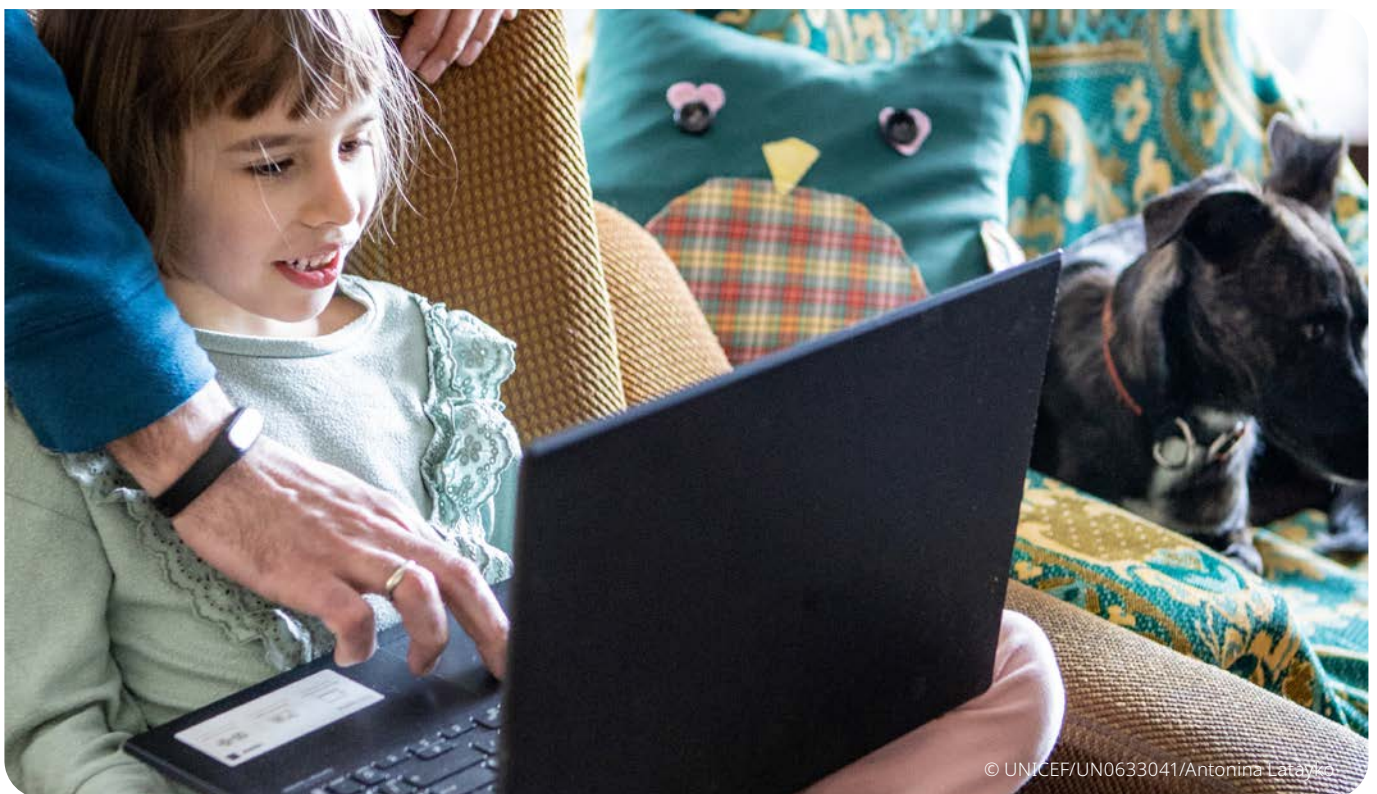
- **Designing systems with clear protocols to detect and respond to unauthorized access** involving children's data, supported by real-time monitoring where feasible. Insufficient monitoring [can allow](#) third-party data extraction to go unnoticed.
- **Implementing child-specific incident response procedures**, including coordination with child protection authorities and notification pathways adapted to children and caregivers.
- **Embedding age-appropriate protections** into child-facing systems, including mechanisms for verifying age and tailoring safeguards to developmental stages.

Key initiative

Responsible Data for Children (RD4C)

The [Responsible Data for Children \(RD4C\) initiative](#), developed by UNICEF and GovLab, provides a **practical framework for improving data governance practices across the full data lifecycle**. The RD4C principles emphasize purpose-driven data collection, proportionality and data minimization, prevention of harm, transparency and participation, and a heightened responsibility when handling children's data.

The [RD4C toolkit](#) offers diagnostic tools and guidance to help governments and organizations to assess their data management practices, strengthen governance structures and ensure responsible, child-centred data practices.



© UNICEF/UN0633041/Antonina Latayko

3.3 Organizational capabilities

- **Defining clear governance roles** for managing risks in systems that store or process children's data, ensuring ownership across leadership, technical teams and actors responsible for service delivery.
- **Conducting ongoing testing and updates** of technical controls, such as simulation exercises for breaches involving children's data.
- **Embedding continuous improvement mechanisms**, incorporating lessons from assessments, incidents and near-misses to strengthen safeguards over time.

- **Investing in staff and partner readiness**, including targeted training in cybersecurity, responsible data handling and third-party risk management.

UNICEF's experiences across contexts suggest that these measures, among others, are **most effective when embedded from the outset, supported by sustained governance, and adapted to the realities** of each environment. These learnings apply not only to individual platforms but also to the large-scale digital public systems that increasingly mediate children's access to essential services.

Key initiative

Applying learnings to Digital Public Infrastructure

Digital Public Infrastructure (DPI) – including identity systems, payments platforms, data exchange layers and other foundational digital services – plays a growing role in how children access health care, education, social protection and legal identity. UNICEF's work with governments reveals that **governance gaps, not only technical design issues, can often create systemic vulnerabilities that affect children.**

UNICEF supports governments in embedding [DPI Safeguards](#) for children, especially related to cybersecurity, data protection and privacy and child rights principles into DPI from the outset. In Lesotho and Tanzania, for instance, UNICEF is supporting the strengthening of civil registration and social protection systems so that they can **interoperate securely and apply appropriate digital protections as they expand**. These experiences reinforce a broader learning: safeguarding children's rights requires secured, well-governed digital foundations at every layer of national systems.



4. Strengthening governance and accountability for digital systems for children

UNICEF's work with partners suggests that many child-serving digital systems remain vulnerable, not only because of technical weaknesses, but also due to **governance and accountability gaps that may leave children's data insufficiently protected**.

Strengthening governance and accountability across public and private actors is increasingly important for ensuring that digital systems uphold, rather than compromise, children's rights.

4.1 For government actors

UNICEF's review indicates that **few national cyber-maturity assessment frameworks explicitly incorporate child-rights considerations**, despite children's data being exceptionally sensitive and often processed at scale in education, health, identity and social protection systems. The [ITU Global Cybersecurity Index](#) remains one of the few global instruments that acknowledge child-specific dimensions of cybersecurity.

To close these gaps, regulatory bodies and governments should:

- **Recognize the heightened risks of handling children's data**, requiring strong protection and minimization.
- **Establish minimum cybersecurity baselines** for child-serving systems, including education, health, civil registration and social protection platforms.
- **Embed child rights risk assessments** into procurement, vendor management and DPI development.
- **Conduct child-focused cyber readiness assessments** to identify vulnerabilities and define remediation actions.
- **Define breach reporting and redress mechanisms for incidents involving children's data**, including appropriate notification to caregivers, and coordination with child protection authorities.

Consistent expectations for child-serving systems can help to reduce fragmentation and improve system resilience. Further research is needed to understand

which governance levers are most effective in different contexts.

4.2 For industry actors

Private sector actors play a defining role in how children's data is secured. UNICEF's work indicates that **incentives to adopt Secure by Design and rights-protecting approaches remain uneven**, and that many widely used digital products may not implement sufficient safeguards for children's information.

Industry actors can safeguard children's rights by:

- **Embedding Secure by Design and Privacy by Design** into system architecture from the outset.
- **Implementing authentication, access management and audit controls** to prevent unauthorized access to children's data.
- **Conducting child rights risk assessments**. UNICEF's [D-CRIA Toolbox](#) provides a structured method for assessing and mitigating risks to children's rights throughout the product lifecycle.
- **Minimizing collection and retention of children's data**, avoiding sensitive or unnecessary data categories by default.
- **Providing accurate, age-appropriate transparency** about how children's data is used, stored and shared.

The goal is not simply to reduce exposure to digital harms, but to ensure that the **technologies powering children's digital lives operate and handle their data securely, responsibly and in line with children's rights**.

4.3 For humanitarian and development actors

Digital threats affecting children (ranging from identity theft to trafficking or system-level breaches) are increasingly transnational. Analyses from the [UNODC](#) and [US Trafficking in Persons Report](#) highlight an increased use of digital networks to identify and target

vulnerable individuals, underscoring the need for stronger cross-border coordination. Effective protection of children's rights in digital systems requires coordinated action across borders and sectors.

Humanitarian and development organizations may protect children's rights by:

- **Applying strict data minimization principles** and avoiding the creation of large, sensitive datasets that can heighten risks for humanitarian and crisis settings.
- **Adopting interoperable technical standards** for secure cross-border exchange of data.
- **Cooperating on breaches involving children's data**, enabling rapid containment and coordinated notification.
- **Strengthening collaboration between stakeholders.** Coordinated action across borders can aid faster detection, attribution and disruption of harmful activities.

UNICEF and partners' experiences indicate that **cross-border collaboration strengthens resilience and helps to close the security gaps** that can be exploited by cyber attackers.

4.4 For all actors

UNICEF's cyber readiness work points that **limited institutional capacity is one of the most persistent barriers** to securing child-serving systems. Governments and humanitarian organizations often struggle with a lack of trained cybersecurity and data governance teams, unclear accountabilities or limited oversight of third-party practices. To address these gaps, they can:

- **Join forces to train civil servants, and local staff and partners** on cybersecurity and responsible data handling for children.
- **Conduct cyber maturity assessments**, including technical capability, governance processes and response readiness.
- **Improve third-party risk management** for systems that process children's information or directly interact with children.

With adequate investment in capacity, systems can become more secure, more resilient and better aligned with children's rights. Across all actors, **information security and data governance frameworks should be treated as core enablers of child rights**, not optional technical enhancements.



5. Conclusion

Children today enter digital systems from the moment they are born – through civil registration, health records, education platforms and social protection services. Yet many of these systems were not designed with children's rights, vulnerabilities or long-term safety in mind. As a result, weaknesses in cybersecurity and data governance controls have direct and lasting consequences for children's well-being, protection and opportunities.

UNICEF's early work through the SafeChild partnership suggests that **strengthening the security and governance of child-serving systems will require sustained investment, clearer accountability and closer collaboration** across governments, industry and humanitarian actors. While promising tools and approaches are emerging, this remains a relatively new field: more research, more evidence and more coordinated action are needed to understand how digital systems can effectively protect and enhance children's rights at scale.

What is already clear is that **technical safeguards alone are not sufficient**. Secure by Design architecture, responsible data governance, capable institutions and child-centred risk assessments all need to work together from the outset. Cybersecurity must be treated not only as an operational necessity, but as a foundational component of child rights protection in the digital age.

Looking ahead, building safe digital futures for children will depend on whether public institutions, the private sector and humanitarian partners invest meaningfully in secured, accountable and rights-respecting digital foundations. By **prioritizing cybersecurity and data governance now**, actors across sectors can help to ensure that the **systems children depend on uphold – rather than compromise – their safety, dignity and agency** in an increasingly digital world.



6. References

5Rights Foundation, 'Our Rights in a Digital World', 11 May 2021, <<https://5rightsfoundation.com/resource/our-rights-in-a-digital-world-full-report/>>.

Burton, Jo, "Doing no harm" in the digital age: What the digitalization of cash means for humanitarian action', March 2021, <<https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/abs/doing-no-harm-in-the-digital-age-what-the-digitalization-of-cash-means-for-humanitarian-action/03763F7BD89280306E44EF0B009A76FE>>

Digital Public Infrastructure Universal Safeguards, <www.dpi-safeguards.org/>.

Government of the United Kingdom Home Office, Department for Science, Innovation & Technology, 'Cyber security breaches survey 2025: education institutions findings', <www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings#chapter-1-overview-of-the-data>.

Human Rights Watch, 'New Evidence that Biometric Data Systems Imperil Afghans', 30 March 2022, <www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans>.

International Committee of the Red Cross, 'Safeguarding Humanitarian Data', May 2022, <https://rcrcconference.org/app/uploads/2022/05/16_CoD22-Safeguarding-Humanitarian-Data-Background-document-FINAL-EN.pdf>.

International Telecommunication Union (ITU), 'Global Cybersecurity Index', <www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx>.

National Institute of Standard and Technology, Cybersecurity Framework, <www.nist.gov/cyberframework>.

Organisation for Economic Co-operation and Development, 'How's Life for Children in the Digital Age?', OECD Publishing, Paris, 2025, <www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/how-s-life-for-children-in-the-digital-age_c4a22655/0854b900-en.pdf>.

Responsible Data for Children, 'Principles', <<https://rd4c.org/principles/>>.

Responsible Data for Children, 'Tools', <<https://rd4c.org/resources/?tab=tools>>.

United Nations Children's Fund, 'Assessing child rights impacts in relation to the digital environment', <www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA>.

United Nations Children's Fund, 'How Lesotho is Protecting Children and Their Families in a Digital Age', 5 December 2025, <www.unicef.org/digitalimpact/stories/how-lesotho-protecting-children-and-their-families-digital-age>.

United Nations Office on Drugs and Crime, 'Trafficking in Persons & Smuggling of Migrants / Cybercrime: Module 14 Links between Cybercrime, Trafficking in Persons and Smuggling of Migrants', <<https://sherloc.unodc.org/cld/en/education/tertiary/tip-and-som/module-14/index.html>>.

United States Department of State, '2024 Trafficking in Persons Report', 2024, <www.state.gov/wp-content/uploads/2025/02/TIP-Report-2024_Introduction_V10_508-accessible_2.13.2025.pdf>.

Published by UNICEF
Digital Impact Division
United Nations Plaza
New York, NY 10017, USA

www.unicef.org

© United Nations Children's Fund (UNICEF), 2026

unicef 
for every child