25th General Assembly Meeting and the Arab Network conference
Protecting Children in the Digital Space: Challenges, Legislation, and Preventive Measures

Working paper:

Technology as a Tool for Protection: Technical Solutions for Preventing Digital Risks for Children

By: Filippo Di Carpegna, UNDP Regional Hub Amman

Executive Summary

Children's lives are increasingly shaped by digital technologies. While online participation offers extraordinary opportunities for learning, creativity and connection, it also exposes children to rapidly evolving risks—privacy violations, manipulative design, cyberbullying, grooming, financial sextortion, and sexual exploitation, including emerging AI-generated content.

International human rights standards—particularly the UN Convention on the Rights of the Child (CRC) and General Comment No. 25 (GC25)—affirm that children's rights apply fully in digital environments. They call on States and on businesses whose activities affect children, to proactively embed protection, privacy and participation, and accountability into technologies by design and by default.

Globally, internet use continues to rise: 68% of the world's population was online in 2024, yet stubborn divides persist by income, geography and gender, disability and age. Youth (15–24) are the most connected demographic (79%), but affordability, skills gaps, and safety concerns continue to limit equitable access, especially in low-income and marginalized settings.

The digital threat landscape is accelerating. The WeProtect Global Threat Assessment 2025 documents sharp growth in AI-generated Child Sexual Abuse Material (CSAM), rapid grooming across social and gaming environments, and persistent financial sextortion—underscoring the urgent need to shift from reactive responses to prevention and safety-by-design.

This paper argues for a shift toward Digital Safety by Design for Children: an approach that embeds safety, privacy, participation, and accountability into digital systems from the outset. Just as physical products and environments used by children are subject to safety standards by design, digital products and services must be engineered to protect children by default.

I. Introduction: Technology as a Tool for Protection

Digital technologies have become integral to children's lives, shaping how they learn, communicate, and participate in society. While these tools unlock unprecedented opportunities for education, creativity, and social connection, they also introduce complex risks—ranging from privacy violations and manipulative design to sexual exploitation and abuse. The central challenge for policymakers, industry, and educators is to ensure that technology functions not merely as a conduit for engagement, but as a proactive mechanism for protection.

When designed with intention, technology can serve as a powerful shield for children in the digital age. Safety-by-design principles—such as high-privacy defaults, age-appropriate interfaces, and proactive detection and mitigation of harmful content—shift the responsibility for safety away from children and caregivers and onto platforms and service providers. This approach recognizes that children experience digital environments differently from adults, due to their developmental stage, limited legal agency, and reliance on systems built primarily designed for adult users.

Across the Arab region, children increasingly rely on digital platforms for education, self-expression, entertainment, and community-building. At the same time, data-driven business models, opaque algorithms, and persuasive design techniques can expose children to surveillance, manipulation, discrimination, economic exploitation, and sexual abuse. These risks are not evenly distributed and often amplified for children in vulnerable or marginalized contexts.

UN Convention on the Rights of the Child (CRC) and General Comment No. 25 (GC25) requires that children's best interests be a primary consideration in the design, governance, and operation of digital services. This includes high-privacy defaults, age-appropriate interfaces, clear and accessible information, and effective systems for detecting and mitigating harmful content and behaviors.

Digital safety by design for children aims to keep children safe while enabling them to benefit fully from the digital environment—just as physical products and spaces for children prioritize safety, so must the digital spaces children inhabit. International human rights standards therefore establish digital safety by design not only as a technical choice, but as a legal, ethical, and governance imperative.

II. Children's Digital Risk Landscape

Digital technologies are now central to children's well-being and development. The digital environment offers significant opportunities for self-expression, learning, socializing, connection with community and culture, and the enjoyment of children's rights. At the same time, it presents a wide spectrum of risks to which children are more vulnerable than adults, including exposure to harmful or illegal content, cyberbullying, breaches of privacy, commercial exploitation, and serious crimes such as sexual exploitation and abuse.

As digital technologies advance, so do the possibilities for design flaws, unintended consequences, and intentional misuse. The risk of exposure to well-recognized harms is accelerating, particularly in relation to online child sexual exploitation and abuse. Emerging technologies, including generative AI, create new vectors for harm while increasing the scale and speed at which abuse can occur.

Children experience digital risks differently from adults due to their developmental stage, limited legal agency, and dependence on platforms primarily designed for adult users. **Key risk categories include:**

- **Content risks:** exposure to age-inappropriate, violent or misleading material.
- **Contact risks:** cyberbullying, harassment, grooming and unwanted interactions.
- **Conduct risks:** children's participation in harmful behaviours without full understanding.
- **Data & privacy risks:** excessive data collection, profiling and targeted advertising.
- **Design risks:** addictive features, dark patterns and persuasive design exploiting vulnerabilities.

These risks are often intensified by opaque algorithms, commercial incentives that prioritize engagement over well-being, and weak accountability mechanisms.

III. Defining Digital Safety by Design

Digital Safety by Design refers to the intentional integration of child safety and children's rights principles into the architecture, functionality, and governance of digital technologies across their full lifecycle.

Rather than relying primarily on reactive moderation or parental supervision alone, this approach embeds protections directly into systems—ensuring that children are safe by default.

Key Components of Digital Safety by Design (for service providers)

- **Employing age assurance mechanisms**: To provide age-appropriate experiences, digital service providers need to know which of their users are children. Age assurance is important for this purpose, but consideration should be given to potential solutions' accuracy, usability, privacy preservation, and risk proportionality.
- **Implementing child-centred design:** Child-centred design puts the evolving needs, preferences, and safety of children at the core of product and service development. This approach aims to ensure that digital products and services are not only accessible and engaging for young users, but inherently safe and beneficial, and that they remain so as children mature.
- **Detecting and preventing harm:** Digital service providers can proactively identify and mitigate risks by implementing technical safety measures, such as advanced detection systems, default settings, content filters, and real-time monitoring tools. Specific attention should be paid to the risks posed by such measures and to their compliance with existing regulations.
- **Protecting children's privacy and personal data:** Breaches of children's privacy and misuse of their data can directly affect their safety. Accordingly, when digital service providers prioritize privacy by design and offer clear privacy settings, it advances safety by design.
- **Ensuring child-friendly information provision:** Children need to understand the digital spaces they inhabit. Consequently, they need clear, timely, accessible, and age-appropriate information about how digital services work, the risks involved, and how they can be protected.
- **Facilitating complaints and redress:** Empowering children to voice concerns and seek remedies is crucial. By establishing clear, user-friendly, accessible, and age-appropriate channels for reporting issues and ensuring timely and effective responses, service providers demonstrate a commitment to children's safety and help uphold trust in the digital ecosystem.
- **Encouraging child participation and putting children at the center of decision-making:** Children are active digital citizens, and both service providers and policymakers should involve them in discussions about online safety, design processes, and policy formulation. By giving children a seat at the table, stakeholders can help ensure that the digital environment is shaped with children's best interests at heart.
- **Promoting a culture of safety and well-being:** Promoting a culture of safety and well-being is essential to developing a responsible corporate culture that prioritizes children's safety.

IV. Examples "By Design" Approaches

1. Designing for Safety Offline

Embedding safeguards into products and services at the level of design is not a new concept. In the offline world, safety by design is widely accepted as a baseline expectation rather than an optional enhancement. Features such as seat belts, airbags, and anti-lock braking systems in cars are now standard examples of safety by design.

In the offline context, designing for safety includes rigorous testing prior to market release, such as clinical trials for pharmaceuticals or safety certification for aircraft. It also includes clear, accessible safety information for consumers, including warnings, labels, and instructions for safe use. Finally, it involves independent oversight and regulatory approval, ensuring that products meet established safety standards before reaching users.

For children, specific safety requirements are routinely mandated for both products designed specifically for children and products that may foreseeably be used by them. Examples include child-resistant packaging for hazardous substances and toy safety standards that limit physical, chemical, and auditory risks. **The European Union's Toy Safety Directive** illustrates this approach through obligations for pre-market testing, risk mitigation, age-appropriate labeling, and communication of safety information in language children and caregivers can understand.

These offline practices demonstrate that designing for safety is a normative and enforceable expectation, providing a clear analogue for digital environments.

2. Digital by design concepts

Applying a "by design" approach to the digital sphere is not new. Digital by design concepts aim to harness the influence of digital service providers, designers, and policymakers to shape product and service development in ways that prioritize values that promote human well-being, rights protection, and accountability. Two well-established approaches—privacy by design and security by design—offer relevant lessons for digital safety by design for children.

A. Privacy by Design

Privacy by design refers to embedding privacy protections by default into the design, operation, and management of organizations, as well as in products and services. **Ann Cavoukian** articulated seven foundational principles for privacy by design:

- Proactive not reactive – preventive not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive sum, not zero sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

In practice, privacy by design has been translated into binding legal obligations. For example, the EU's General Data Protection Regulation (GDPR) requires data protection by design and by default, reinforcing the principle that privacy protections must be built into systems from the outset rather than retrofitted.

B. Security by Design

Security by design involves building cybersecurity protections into digital products and services from their earliest development stages. It seeks to ensure that systems reasonably protect against unauthorized access, misuse, and malicious actors across devices, infrastructure, and data flows.

While no system can be secured permanently, products that lack security by design are demonstrably more vulnerable to exploitation, increasing risks for all users, including children.

C. Shared Principles Relevant to Digital Safety by Design for Children

Despite differences in focus, privacy by design and security by design share several characteristics that are directly applicable to digital safety by design for children, including:

- **Baseline safeguards** (e.g., minimization, safe defaults, ban on harmful dark patterns).
- **Risk/impact assessments** across the lifecycle.
- **Accountability** through roles, governance and audit.
- **User-centricity** with understandable controls and rights.
- **Transparency** (clear information, reporting, vulnerability disclosure).

3. Applying a digital, by design approach to children

Beyond safety, children's rights advocates have developed frameworks that apply by-design thinking to children's unique needs in the digital environment. These include children's rights by design and playful by design, both promoted by **the Digital Futures Commission**.

a. Children's rights by design

This concept situates the protection of children within a holistic framework of children's rights encompassing protection of life, non-discrimination, participation, privacy, and information, amongst others. This guidance is for innovators of digital products and services that are likely to be used by, or likely to affect children, to support the practical implementation of rights by design.

The guidance is underpinned by eleven principles: i) equity and diversity; ii) best interests; iii) consultation; iv) age-appropriateness; v) responsibility; vi) participation; vii) privacy; viii) safety; ix) wellbeing; x) development; and xi) agency. The principles of equity and diversity, best interests, age appropriateness, and privacy are noted as key to enhancing children's safety in the digital environment. The resource recognizes that collectively these principles promote safe, inclusive, and age-appropriate content whilst protecting children's personal data from exploitation. Additionally, it emphasizes that responsibility and safety in design can help create safe digital spaces, actively mitigating potential risks.

b. Playful by design

Playful by design is a tool that aims to help designers enhance children's opportunities for play in the digital environment and address the challenge of developing digital products and services that respect children's rights. It also seeks to support parents and game reviewers to evaluate the opportunities for free play in digital games. The tool includes resources to initiate discussion and provoke reflection and fresh ideas. It is directed at any stakeholder developing digital products and services used by children and can be used at any stage of the design process.

The playful by design tool is made up of cards that prompt child-focused thinking by designers and other stakeholders. They are grouped in the following categories: i) be welcoming; ii) enhance imagination; iii) support open-ended play; iv) adopt an ethical commercial model; v) ensure safety; vi) allow for experimentation; and vii) be age appropriate.

Together, these approaches reinforce that intentional design choices shape whether digital environments support or undermine children's rights and safety.

V. International Initiatives & Policy Guidance

While no universally accepted definition of digital safety by design for children exists, the concept is firmly embedded in international human rights and policy frameworks.

The UN Committee on the Rights of the Child, in its **General Comment 25**[1], recognizes that digital safety by design is necessary for fully protecting children's rights in the digital environment. It recommends that safety by design be integrated into the services and products that children use, so as to minimize the risks they face in the digital environment. An Explanatory Note to General Comment 25 states that safety by design is the practice of designing services with the goal of ensuring users' safety, for instance by default safe settings for accounts of underage users or by preventing adults from contacting children.

General Comment No. 25 recommends that states require businesses whose activities affect children's rights in the digital environment to implement regulatory frameworks, terms of service, and industry codes that adhere to the highest standards of safety, ethics, and privacy in relation to the design, development, engineering, operation, distribution, and marketing of their products and services. It further recommends that businesses maintain high standards of accountability and transparency and encourages them to take measures to innovate in the best interests of children. Lastly, it sets out that businesses should require the provision of age-appropriate explanations of their terms of service to children, or to parents and caregivers for very young children.

The **CRC** provides fundamental principles and rights that should be applied systematically both to promote children's rights and development and to protect them from violations regarding the detrimental use of their data.

Principle	Description
Best Interests of the Child	All use of children's data must prioritize their best interests (Art. 3.1), guiding actions by companies and data holders—even when processing is legally justified.

[1] CRC GC No. 25 (2021), OHCHR. [ohchr.org]

Evolving Capacities & Participation	Design and development should respect children's evolving capacities (Art. 5) and allow them to be heard in the process (Art. 12.2).
Sensitive Data	Children's data must always be treated as sensitive, including genetic, biometric, criminal, racial, political, religious, health, or sexual information.
Non-Discrimination & Equal Protection	Children's data must not be used to discriminate or perpetuate bias. Advanced protection technologies should be universally adopted for all children without discrimination (Art. 2).
Right to Privacy & Data Ownership	Children have the right to privacy (Art. 16), confidentiality of communications, and full ownership of their data, including the right to erase it at any time.
Protection from Violence & Exploitation	Children must be safeguarded from all forms of abuse and exploitation in digital environments (Art. 19.1), including risks from data processing and exposure.
Protection from Economic Exploitation	Children must be protected from commercial exploitation of their data (Art. 32.1), including profiling, targeted ads, and monetization of personal content.
Freedom of Expression & Thought	Children's rights to expression (Art. 13.1) and thought (Art. 14) must be upheld, preventing manipulative algorithms and opaque decision-making.
Rights to Development, Health, Education & Play	Data use should support children's holistic development (Art. 6.2), health (Art. 24), education (Art. 28), and leisure/play (Art. 31), including the right to disconnect.
Business Model Transformation	Exploitative models must be replaced with educational, transparent designs promoting citizenship and identity (Art. 8). Children should access diverse information (Art. 17) and safe, commercial-free spaces (Art. 15).

The UN General Assembly Resolution on the Rights of the Child in the Digital Environment[2] encourages states to urge companies to address negative effects on children's rights in the digital environment that are associated with their design, operations, products, and services. It calls for the promotion of industry codes and terms of service that respect, protect, and fulfil the rights of the child and uphold ethics, privacy, and safety standards in relation to the design, engineering, development, operation, distribution, and marketing of technological products and services. It encourages private actors in the technology sector to take into account the particular needs of children and follow international standards and best practices for safety, privacy, and security by design.

UNICEF research[3] notes that digital safety by design for children should include taking preventative measures to make sure that anticipated and known harms have been evaluated in the design and provision of a digital service. This research also underlines that user empowerment, and autonomy should be secured as part of an in-service experience, that organizations should take ownership and responsibility for user safety, and that they should be transparent about the measures taken to address any concerns.

The OECD Recommendation[4] encourages governments to promote safety by design through fostering the research, development, and adoption of privacy-protective, interoperable, and user-friendly technologies that can restrict contact and access to content inappropriate for children, taking into account their age,

[2] UNGA Resolution on Rights of the Child in the Digital Environment (A/RES/78/187, 2023). [digitallib…ary.un.org]
[3] The children's rights-by-design standard for data use by tech companies, Pedro Hartung, UNICEF.
[4] OECD – Towards Digital Safety by Design for Children (2024). [oecd.org]

maturity, and circumstances (at III.5.a). It also calls for providing all stakeholders with clear information as to the trustworthiness, quality, user-friendliness, and privacy by design of such technologies (at III.5.b). The OECD Guidelines advise digital service providers to take a child safety by design approach in designing, delivering, and deploying services that are either directly intended for children or where it is reasonably foreseeable that they will be accessed or used by children.

The Council of Europe's (CoE) Guidelines[5] to respect, protect, and fulfil the rights of the child in the digital environment note the importance of safety by design for children. These guidelines call upon CoE member states to promote safety by design and to provide incentives to businesses to implement it as a guiding principle for products' and services' functionalities and features that might be used by children or addressed to them.

The International Telecommunication Union (ITU) Guidelines for industry on Child Online Protection[6] recommend that, to create a safe and age-appropriate digital environment, companies should always consider safety by design in products and services that are addressed to, or commonly used by, children. These guidelines stress that children's safety and the responsible use of technology should be carefully considered and not be an afterthought.

The **WeProtect Global Alliance Global Threat Assessment** (2023)[7] Highlights escalating risks including financial sextortion, rapid grooming in gaming environments, and AI-generated abuse imagery, reinforcing the urgency of design-based prevention

VI. The Arab Regional Context: Laws, Policies, and Initiatives

In the Arab region, reliance on parental consent and digital literacy initiatives alone has proven insufficient to address systemic risks faced by children online. Design choices, opaque algorithms, and data-driven business models often shift responsibility for safety onto families with limited bargaining power.

Encouraging developments across the region include:

- **League of Arab States & UNICEF MENA – "Safe Internet for Our Children" (Phase II, 2025):** Regional awareness campaign with multilingual content and **"Alpha & Zein"** episodes on digital ethics, cyberbullying, screen balance and misinformation.
- **ITU Arab States Child Online Protection** programmes support national and regional efforts to safeguard children online, with **Egypt** hosting the Amanak Portal as a regional repository and dialogue platform, and Oman implementing **OCERT COP**, which combines a national strategy with workshops and awareness campaigns to promote safe and responsible digital use among children.:
- **United Arab Emirates (2025): Federal Decree-Law on Child Digital Safety.** Establishes a comprehensive framework applying to platforms operating in or targeting the UAE; creates a **Child**

[5] Guidelines to respect, protect and fulfil the rights of the child in the digital environment Recommendation CM/Rec(2018)7 of the Committee of Ministers, CoE - https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a
[6] ITU Guidelines for Industry & Policy-Makers on Child Online Protection (2020). [itu.int], [itu.int]
[7] WeProtect Global Threat Assessment 2025. [weprotect.org]

Digital Safety Council (chaired by the Minister of Family); introduces platform classification by risk and **age-based controls**; places obligations around privacy defaults and data restrictions for children under 13.

- **Jordan (2022–2024): Child Rights Law (2022)** protects privacy and participation; national study (NCFA/Save the Children, 2024) highlights enforcement gaps and calls for stronger age-verification and reporting systems addressing cybercrimes against children.
- **Saudi Arabia (2014–2024): Child Protection Law** and **Personal Data Protection Law (PDPL)** require safeguarding minors and lawful processing; Saudi Arabia's UN engagement (2025) called for enhanced capacity to protect children in cyberspace.
- **Egypt (2024–2025): Digital Citizenship & Online Safety Initiative (MCIT)**—national awareness and training with UNICEF, expanding via public libraries, schools and youth centers; NCCM maintains national child protection helpline and support services.
- **Morocco (2024): E-Blagh**—national DGSN portal enabling citizens to report illegal content including threats to minors' rights; integrated into DGSSI incident reporting guidance; thousands of reports processed in first months.
- **Tunisia (2025): National Charter for a Child-Safe Digital Environment**—multi-stakeholder framework across ministries, ISPs, telecom operators and media to empower families and strengthen prevention/response to online violence against children.

VII. Case Study: LEGO® Life — A child-centred social app

LEGO's Life App

LEGO Life is a social media application designed for children to share stories and pictures of their LEGO creations. Children can access interactive building ideas and instructions and comment on other users' photos.

Digital Safety by Design Components:

- **Employing age assurance mechanisms:** When children attempt to create an account on LEGO Life, they are asked to provide a parent's email address. LEGO then sends an email to the parent to inform them of the account creation attempt and requests consent. This serves as a form of age verification and parental supervision. In addition, an age-gate prompts users to declare age. To reduce the incentive to lie, children can still enjoy a "boxed" version of the app if parental consent is not received—with fuller social features unlocked once verifiable parental consent is achieved.
- **Implementing child-centered design:** Given its audience, the LEGO Life App's features are child-centered, allowing children to be creative and engage in digital play.
- **Detecting and preventing harm:** Moderators review all posts to ensure they do not include any personal information and that they are age-appropriate.
- **Protecting children's privacy and personal data:** Children can choose from pre-approved, auto-generated usernames and create their LEGO avatar to remain anonymous, without sharing personal information. The company states that it follows standards of data privacy

and security in accordance with the GDPR anywhere in the world where it collects, stores, uses, or shares users' personal data. Where local rules require more than that, the company states it will adjust its practice to ensure users' data is safe.

- **Ensuring Child-Friendly Information Provision** A tool within the Life App called **"Captain Safety"** provides guidance for children on behaving like responsible digital citizens. All users learn how they should behave appropriately through a safety pledge and receive periodic reminders as they engage with the app. Captain Safety also explains moderation and safety decisions to children (e.g., why they need to be thoughtful when uploading images) and helps them understand LEGO's privacy policies.
- **Facilitating complaints and redress:** No specific complaint and redress information is specified.
- **Encouraging child participation and putting children at the center of decision making:** No information is available on child participation and putting children at the center of decision making.
- **Promoting a culture of safety and well-being:** LEGO launched Digital Design Principles that prompt designers in the LEGO Group to consider children's perspectives and needs through strategic, design, and engagement lenses. Children sign a code of conduct that includes topics such as "I will protect my privacy" and "I will be kind to others." Tools and articles address topics such as safety and privacy and promote digital literacy.
- **Additional Features:**
  - Parental tools are included in the app. For example, verified parental consent enables parents to verify their identity and give consent for their children to play and share within the application.
  - Through certain exercises, the Life App guides children to ensure they are aware of their own and others' feelings and helps them develop empathy.

Risk Profile

LEGO's Life App incorporates child-centric design, strong moderation features, and a capacity for parents, carers, and guardians to monitor their child's usage. However, as zero risk is unattainable, there remains potential exposure to risks such as:

- **Content risks:** Even with moderation in place, there is always a chance that inappropriate content might affect children. Whilst LEGO employs moderators to review uploads, human and algorithmic methods can occasionally miss harmful content.
- **Privacy risks:** As with any app that collects data, there remains concern that data may be accidentally shared or subject to a data breach (Valentino-DeVries and Singer, 2018[150]).

Although LEGO's Life App is safer than many other platforms due to its child-centric design and strong moderation features, parents, carers, and guardians should still monitor their child's usage, ensuring they maintain a balanced approach to both digital and physical experiences.

VIII. Recommendations

For Governments

1. Legislate for safety-by-design and privacy-by-default for services accessed by children; require child-rights due diligence and lifecycle risk assessments.
2. Mandate age assurance that is accurate, proportionate and privacy-preserving; ban profiling-based ads to minors; tackle dark patterns.

3. Establish independent regulators (or expand mandates) with co-regulatory codes, audits and enforcement powers; support cross-border cooperation.
4. Build national reporting & remedy mechanisms (hotlines, assistance, victim support) designed for children; integrate with CSAM hash-sharing alliances and Lantern.
5. Fund research and data on children's digital experiences; monitor enforcement outcomes and equity impacts (gender, rural/urban, disability).

For National Human Rights Institutions (NHRIs)

1. Normative Guidance and Alignment**:** Issue NHRI guidance clarifying how the CRC, General Comment No. 25, and relevant UN resolutions apply to digital services used by children, including safety-by-design and privacy-by-default obligations.
2. Child-Rights Due Diligence: Promote the systematic use of child-rights impact assessments for digital services likely to affect children, including risks related to design, data use, algorithms, and AI, across the technology lifecycle.
3. Oversight and Accountability: Monitor State and platform compliance with child digital rights standards and publish child-specific transparency findings, including risk management practices and redress effectiveness.
4. Complaint, Remedy, and Support: Establish or support child-friendly, trauma-informed reporting and remedy mechanisms, linked to legal aid, psychosocial support, and referral pathways, including cross-border cooperation where relevant.
5. Child Participation: Institutionalize mechanisms for meaningful child participation in digital policy, platform oversight, and remedy design, in line with children's evolving capacities.
6. Coordination and Co-Regulation: Convene regulators, platforms, civil society, and youth to support co-regulatory approaches and sector-specific standards (e.g. social media, gaming, edtech) that embed safety by design.
7. Regional Cooperation and Evidence: Strengthen regional coordination among Arab NHRIs, including information sharing, joint responses to cross-border harms, and the generation of evidence and data on children's digital experiences.
8. Capacity Building and Prevention: Support capacity building for public institutions and key stakeholders on child digital rights, safety-by-design approaches, and trauma-informed responses, alongside rights-based public awareness initiatives.
9. Public Awareness: Partner with LAS/UNICEF to amplify Alpha & Zein content and adapt for local languages; scale digital citizenship campaigns through schools, libraries and youth centers.

For Civil Society Organizations (CSOs)

1. Monitor and expose design-based harms: Track and document how platform design, algorithms, and data practices create risks for children; use evidence to advocate for reform.
2. Build technical literacy for advocacy: Strengthen CSO capacity on platform architecture, AI risks, and data governance to enable informed rights-based engagement with regulators and industry.
3. Empower children beyond awareness: Deliver digital literacy programmes that help children understand system-level risks, exercise agency, and access remedies—not just "safe behavior" guidance.
4. Provide survivor-centred support: Offer confidential, child-friendly support and referral pathways for victims of online abuse, exploitation, and digital rights violations.

5. Convene multi-stakeholder dialogue: Facilitate collaboration between children, policymakers, educators, and platforms; promote regional cooperation and sharing of good practices.

For Businesses & Platforms

1. Adopt child-centred design with high-privacy defaults; minimize data collection and retention.
2. Implement proactive detection/mitigation for grooming, sextortion and CSAM, with careful safeguards; participate in Lantern.
3. Provide child-friendly terms, notices and controls; enable trusted reporting and redress; publish transparency reports on harms and actions.
4. Conduct child-rights impact assessments and independent audits; assign executive accountability for child safety.

For Schools & Caregivers

1. Integrate digital citizenship and online safety into K–12 curricula, tailor content to age and evolving capacities.
2. Use privacy-respecting parental controls and foster open dialogue about risks and resilience.

IX. References

- CRC GC No. 25 (2021), OHCHR. [ohchr.org]
- UNGA Resolution on Rights of the Child in the Digital Environment (A/RES/78/187, 2023). [digitallib…ary.un.org]
- ITU Facts & Figures 2024; Youth Internet Use. [itu.int], [itu.int]
- OECD – Towards Digital Safety by Design for Children (2024). [oecd.org]
- WeProtect Global Threat Assessment 2025. [weprotect.org]
- ITU/UNICEF Guidelines for Industry & Policy-Makers on Child Online Protection (2020). [itu.int], [itu.int]
- Guidelines to respect, protect and fulfil the rights of the child in the digital environment Recommendation CM/Rec(2018)7 of the Committee of Ministers, CoE
- EU Digital Services Act and children's safeguards. [eur-lex.europa.eu], [eur-lex.europa.eu]
- Ofcom Online Safety guidance & codes (2024–2025). [ofcom.org.uk]
- Technology Coalition – Lantern (program & transparency reports). [technology…lition.org], [technology…lition.org]
- LAS/UNICEF MENA – "Safe Internet for Our Children" (Phase II). [wam.ae]
- ITU Arab States COP – Amanak; Oman OCERT COP. [itu.int]
- UAE Federal Decree-Law on Child Digital Safety (2025). [wam.ae]
- Jordan NCFA / Save the Children study (2024). [jordannews.jo]
- Saudi Child Protection Law & PDPL; SPA statement (2025). [boe.gov.sa], [sdaia.gov.sa], [spa.gov.sa]
- Egypt MCIT Digital Citizenship initiative; NCCM services. [mcit.gov.eg], [nccm.gov.eg]
- Morocco E-Blagh (DGSN) & DGSSI. [dgssi.gov.ma], [medias24.com]
- Tunisia National Charter (2025). [techafricanews.com]
- LEGO Life & UNICEF partnership (COSA/RITEC). [lego.com], [apps.apple.com]