

# Building a digital environment designed with children in mind

An international best practices blueprint



**In 2021, UNCRC General comment No. 25 offered the world a roadmap to realize in the digital world the rights enshrined in the most widely ratified human rights treaty in history: the UN Convention on the Rights of the Child.**

Significant progress has followed. Across every continent, multilateral, regional, and national institutions have begun enshrining age-appropriate design standards and holding tech companies accountable for respecting children's rights by design and default. Evidence demonstrates that when laws require it, tech companies make meaningful changes: they increase privacy protections in children's default settings, redesign recommender systems, and restrict targeted advertising to children.

Yet, the digital environment children grow up in remains inconsistent. While some jurisdictions have established strong protections, children using the same products and services elsewhere face a plethora of risks. Tech companies frequently continue to design digital products and services that maximize profit at children's expense by systematically amplifying content, contact, conduct, and contract risks.

One in three internet users is a child, and digital technologies increasingly mediate all aspects of their lives. Five years of implementing UNCRC General comment No. 25 have built a solid evidence base demonstrating that embedding age-appropriate design delivers concrete, measurable improvements to children's experiences.

## How does the digital world expose children to risks and harms?

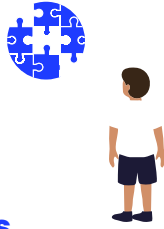
Technology is not neutral – it reflects the values, biases, and priorities of those who design and deploy it. When tech companies prioritize commercial interests and profit at the expense of children's rights and wellbeing, they create digital environments that exploit children's distinct psychological triggers – social anxiety, fear of missing out, and the need for validation among others – through manipulative design choices, including infinite scroll, autoplay, oversized opt-in buttons, ephemeral content, and constant notifications.

This exposes children to harmful material, commercial surveillance, compulsive behaviour, and other risks undermining their rights in tech companies' pursuit of profit. Addressing these harms requires moving beyond surface-level and incomplete solutions.

**Read the entire report**



 **5RIGHTS  
FOUNDATION**



## Incomplete approaches

Content removal, digital literacy, or so-called ‘user empowerment’ responses address the most egregious and visible symptoms rather than the root causes. This type of legislation ignores how companies’ systemic design choices – such as algorithmic amplification, engagement-driven business models, and opaque recommendation systems – deliberately exploit children’s distinct vulnerabilities.

## Fundamental Principles for the systemic protection of children

To effectively protect children in the digital world, regulatory frameworks must shift towards systemic risk management that requires tech companies to proactively assess and mitigate how their products may expose children to risk, allowing them to safely enjoy the full benefits of the digital world.

This approach is already the standard across several industries from food safety to aviation and medicine, where products cannot reach the market without demonstrating safety.

Building on best practices that have emerged at the global, regional, and national levels, this blueprint sets out 10 mutually reinforcing regulatory principles to address harmful design and business models, strengthen accountability, and ensure technology is safe and age-appropriate by design and default.



**1**

Explicitly protect children, as every individual below the age of 18.

**2**

Protect children across all digital spaces they are likely to access or be impacted by.

**3**

Make children’s best interests a primary consideration.

**4**

Require age assurance to provide children with age-appropriate experiences.

**5**

Mandate Child Rights Impact Assessments (CRIAs).

**6**

Embed privacy and safety by design and default.

**7**

Prohibit practices likely to contribute to known harms.

**8**

Ensure published terms are available, age-appropriate, and upheld.

**9**

Mandate responsible business conduct.

**10**

Establish effective enforcement mechanisms.