

Policy brief

Online safety & platform accountability

Strengthening child protection
in the digital age

June 2026



POLICY BRIEF

ONLINE SAFETY AND PLATFORM ACCOUNTABILITY

JUNE 2026

Strengthening Child Protection in the Digital Age

Target Audience: International Regulators, Technology Companies, National Governments, Development Partners, and Media

Scope: Global Digital Governance and Child Protection Systems

CONTEXT

As digital economies expand globally, children are increasingly exposed to technology-facilitated harms including online child sexual exploitation and abuse (OCSEA), grooming, sextortion, cyberbullying, trafficking, and exposure to harmful content. While digital technologies present opportunities for learning, participation, and innovation, they have also created rapidly evolving environments where violence against children can occur at unprecedented scale and speed.

Findings from the Out of The Shadows Index (OOSI), alongside national pledge mapping across countries, reveal growing political recognition of online harms affecting children. However, implementation of child online safety frameworks remains fragmented, underfunded, and uneven across jurisdictions.

Although several governments have introduced online safety legislation and platform regulation measures, significant enforcement, coordination, and accountability gaps persist. Technology companies continue operating across borders while child protection systems remain constrained by inconsistent legal frameworks, weak regulatory cooperation, and limited survivor-centered response mechanisms.

Online safety must therefore be approached not only as a technology issue, but as a child rights, governance, and justice imperative. Effective digital governance systems must be rights-based, survivor-informed, and inclusive by design, ensuring that children – including children with disabilities and historically excluded groups – are protected within rapidly evolving digital environments.

This brief aligns with:

- The United Nations Convention on the Rights of the Child (UNCRC)
- General Comment No. 25 on Children’s Rights in the Digital Environment
- The African Union Child Online Safety and Empowerment Strategy
- The INSPIRE Framework for Ending Violence Against Children
- Sustainable Development Goals 5, 10, 16, and 17
- WeProtect Global Alliance commitments on online child safety

KEY FINDINGS

- National pledge mapping across priority countries reveals growing political recognition of online harms affecting children, but uneven implementation of child online safety frameworks.
- Child protection systems remain underfunded and poorly coordinated across jurisdictions.
- Cross-border digital exploitation continues to outpace existing legal and enforcement mechanisms.
- Survivors and children continue to face inaccessible reporting systems and limited survivor-centered support services.

THE CHALLENGE

Voluntary corporate compliance has proven insufficient in securing today’s borderless digital ecosystem. While some high-income countries continue developing domestic online safety regulations, global technology platforms still largely treat child protection as a discretionary design feature rather than a binding statutory obligation.

The absence of harmonized international standards allows perpetrators to exploit cross-border legal and enforcement gaps, exposing children – particularly those in low- and middle-income countries – to escalating forms of technology-facilitated sexual exploitation and abuse with limited accountability.

Unlike many forms of offline violence, online exploitation frequently involves transnational networks operating across jurisdictions. Effective prevention and response therefore require coordinated international cooperation, harmonized legislation, and enforceable accountability systems between governments, regulators, law enforcement agencies, and technology companies.

Key structural barriers continue to undermine child online safety:

1. Regulatory Fragmentation

National legal frameworks remain inconsistent and poorly coordinated, limiting governments' ability to regulate global platforms effectively.

2. Weak Platform Accountability

Many technology companies lack transparent child safety obligations, independent oversight mechanisms, and meaningful accountability for harmful design failures.

3. Underinvestment in Protection Systems

Child protection agencies, cybercrime units, educators, and frontline responders often lack the resources and technical capacity to respond effectively to online harms.

4. Limited Survivor-Centered Approaches

Reporting systems remain inaccessible, retraumatizing, and poorly adapted to the realities faced by children and survivors navigating digital abuse.

5. Digital Inequality

Children in marginalized, low-connectivity, and underserved communities face heightened exposure to online exploitation while simultaneously lacking access to digital literacy and protection resources.

STRATEGIC RECOMMENDATIONS

For Governments and Regulators

1. Develop and strengthen comprehensive national online safety frameworks grounded in child rights and survivor protection principles.
2. Establish mandatory platform accountability obligations including:
 - child risk assessments,
 - transparency reporting,
 - rapid harmful content response systems,
 - and independent regulatory oversight mechanisms.
3. Harmonize cross-border legislation and strengthen international cooperation mechanisms addressing online child sexual exploitation and abuse.
4. Invest in specialized cybercrime, child protection, and digital investigation units with trauma-informed and survivor-centered protocols.
5. Embed child online protection across national digital transformation, education, and cybersecurity strategies.
6. Prioritize preventative approaches including digital literacy, caregiver awareness, school-based online safety education, and early intervention systems that reduce children's vulnerability to online harms.

For Technology Platforms

6. Adopt safety and inclusion by design standards across all digital products and services.
7. Strengthen multilingual, child-friendly, and accessible reporting mechanisms for children, caregivers, and frontline responders.

8. Improve transparency regarding detection, reporting, moderation, and removal of online child exploitation material.
9. Conduct regular independent child rights impact assessments on digital products, algorithms, and platform systems.
10. Invest in proactive safeguards addressing grooming, sextortion, trafficking, and algorithm-driven exposure to harmful content.

For Donors and Development Partners

11. Increase flexible and long-term financing for child online protection systems, survivor support services, and prevention initiatives.
12. Support regional and global cooperation frameworks addressing cross-border digital harms.
13. Invest in child-centered research, evidence generation, and survivor-informed policy innovation addressing emerging online risks.
14. Strengthen digital literacy and online safety education for children, caregivers, educators, and frontline practitioners.

THE MOMENT TO ACT

As governments prepare national pledges ahead of the 2nd Ministerial Conference on Ending Violence Against Children, the opportunity to strengthen online safety systems has never been more urgent. Governments, regulators, technology companies, and development partners must act collectively to ensure that children are protected within rapidly evolving digital environments.

Key priorities for immediate action include:

- Child protection cannot remain secondary to digital expansion.
- Online safety must be treated as a child rights and justice imperative.
- Platform accountability should move from voluntary compliance to enforceable regulation.

- Harmonized cross-border cooperation is essential to addressing transnational online abuse.
- Survivor participation must be institutionalized within digital governance and child protection systems.
- Sustainable financing for online safety prevention and response mechanisms is a governance responsibility, not an optional investment.
- Safety and inclusion by design should become standard practice across digital products and platforms.
- Governments and technology companies must prioritize child-centered, rights-based, and survivor-informed approaches in all digital policy frameworks.

“Child protection cannot remain secondary to digital expansion.”

Source: [Out of The Shadows Index](#)