GENEVA CENTRE FOR HUMAN RIGHTS ADVANCEMENT AND GLOBAL DIALOGUE

DIPLOMATIC BREAKFAST REPORT

3 SEPTEMBER 2026

Growing Up Online: Protecting Children's Rights in the Digital Age

From Restriction to Rights-Based, Safe and Meaningful Digital Participation.



Growing Up Online:
Protecting Children's Rights in the Digital Age

Moving from Restriction to Rights-Based, Safe and Meaningful Digital Participation

Executive Summary

Digital technologies are increasingly embedded in children's everyday lives, creating significant opportunities for participation, education, connectivity and access to information, while also exposing children to new and evolving risks. Artificial intelligence (AI) and rapidly evolving digital technologies are fundamentally reshaping the environments in which children learn, communicate, access information and develop relationships. While these technologies offer significant opportunities for education, participation and connectivity, they also amplify existing risks and create new forms of harm. The international framework for protecting children's rights in the digital environment is increasingly well established. The Convention on the Rights of the Child applies online as it does offline, and General Comment No. 25 provides comprehensive guidance on children's rights in relation to the digital environment. The Global Digital Compact has further reinforced commitments to strengthen legal and policy frameworks for children's rights and safety online.

The central challenge is therefore no longer primarily the absence of standards, but their implementation. Children's online safety cannot be achieved through prohibition, surveillance or parental controls alone. Broad restrictions can be circumvented, may push children towards less regulated spaces, and can undermine other rights, including privacy, access to information, freedom of expression and participation.

At the same time, responsibility for online safety should not be placed primarily on children and families. Many of the risks children encounter are shaped by deliberate design choices and commercial incentives. Technology companies therefore have a responsibility to integrate child safety and human rights considerations into the design, development and deployment of their products.

A rights-based approach requires moving towards safe-by-design and child-rights-by-design digital environments, supported by effective regulation, meaningful child participation, accountable corporate practices, accessible support systems and stronger national, regional and international cooperation. The objective should not be to keep children away from technology, but to ensure that they can participate in the digital environment safely, meaningfully and with dignity.

1. WHY THIS ISSUE MATTERS TODAY

Digital technologies have become an integral part of children's everyday lives, making the digital environment an essential space for learning, communication, social interaction and participation. For many children, there is no longer a meaningful distinction between their online and offline lives. As a result, protecting children's rights in the digital environment is not about creating a separate set of rights, but about ensuring that existing rights are effectively upheld in a rapidly changing technological context. The Committee on the Rights of the Child's General Comment No. 25, adopted in 2021, reaffirmed that the full range of children's rights applies equally in the digital environment. The Global Digital Compact, adopted in 2024, further recognised the need to strengthen legal and policy frameworks to protect children's rights and safety online. Yet, the central challenge is increasingly one of implementation rather than the absence of principles or guidance.

This implementation gap is particularly significant given the speed at which digital technologies are evolving. Artificial intelligence is developing and being integrated into digital services at a pace that can outstrip the capacity of public institutions to assess risks, regulate emerging technologies and provide effective remedies. The preliminary work of the UN Independent International Scientific Panel has similarly highlighted concerns regarding the ability of institutions to keep pace with technological developments. AI is also increasingly being used in areas that directly affect children, including education, healthcare, welfare and care systems, while AI-enabled products such as companion toys and other services designed for children are entering the market in an environment where appropriate safeguards and regulatory frameworks may not yet be sufficiently developed. This raises fundamental questions about accountability, safety and the need to assess the potential impact of technologies on children's rights before, rather than after, they are deployed.

At the same time, the risks children encounter online cannot be understood solely as unintended consequences of technological innovation. Many are closely connected to how digital services are designed and operated. Features such as infinite scrolling, autoplay, persistent notifications and recommender systems can influence children's online experiences and potentially contribute to harmful patterns of engagement. Commercial incentives and business models can also shape these practices, while companies may apply different safety measures depending on the regulatory environment in which they operate. It is important to highlight this discrepancy: children using the same platform and the same device may benefit from stronger safeguards in one country than in another. Such differences raise questions about how children's rights can be protected consistently across borders and whether safety should depend on the strength of national regulation.

Efforts to protect children online also involve complex trade-offs. Measures such as age restrictions, age assurance and parental controls may contribute to safety in specific contexts, but they raise questions concerning privacy, proportionality, effectiveness and accessibility. Different forms of age assurance—including self-declaration, age estimation and identity verification—have different implications, and the appropriate approach depends on the objective being pursued. Similarly, parental controls may provide useful support for some families but cannot constitute a comprehensive response to the broader structural and systemic risks present in the digital environment. Broad restrictions or bans may also be circumvented, potentially shifting children towards other platforms or less monitored spaces rather than addressing the underlying risks. It is important to highlight that measures are necessary, proportionate, evidence-based and adapted to the specific harm they seek to address.

Another important dimension is the availability of effective support and remedy. Protecting children online cannot be reduced to preventing access to harmful content or restricting the use of particular services. Children may be reluctant to seek help because they fear having their devices taken away, facing punishment from parents or caregivers, or encountering support systems in which they do not have confidence. Effective child protection therefore requires trusted reporting, referral and support mechanisms that recognise children not only as users who need protection, but also as rights-holders whose experiences and perspectives should inform the policies and systems designed to protect them.

Finally, the inherently global nature of the digital environment means that no State can address these challenges alone. National regulation remains essential, but differences between legal and regulatory systems can create uneven levels of protection and allow risks to move across borders. Regional and international cooperation continues to be strengthened through initiatives involving States, United Nations entities and civil society, as well as through ongoing work within the Human Rights Council and other international processes. Regional approaches may also provide opportunities to identify common standards while taking account of different national and regional contexts.

The urgency of the issue therefore lies not in choosing between children's access to technology and their protection, but in ensuring that these objectives reinforce one another. Children should not have to choose between digital participation, safety, their rights and their dignity. The task for policymakers and other stakeholders is to translate established rights and principles into effective safeguards, accountability mechanisms and practical measures that keep pace with technological change—while preserving the significant opportunities that digital technologies can offer to children.

2. Q&A: KEY ISSUES EMERGING

What are the main gaps in protecting children online?

The principal challenge is not the absence of international standards, but their implementation. Existing frameworks need to be translated into effective legislation, regulatory measures, safety-by-design practices and accessible support systems. Governments also face capacity constraints in keeping pace with technological developments.

Are social media bans and age restrictions effective solutions?

Blanket bans are not a comprehensive solution. Children may circumvent restrictions using VPNs or migrate to less monitored platforms. Age-assurance measures should be tailored to clearly identified risks, proportionate to their objectives and designed to minimise the collection of personal information.

Who should be responsible for children's online safety?

Responsibility must extend beyond children and their parents. Governments should establish and enforce effective regulatory frameworks, while technology companies must integrate safety features into products from the design stage. Parents, educators, civil society and children themselves also have important roles in prevention, education and support.

How can children's safety be balanced with other fundamental rights?

Protective measures must respect children's rights to privacy, freedom of expression, access to information and participation in the digital environment. Measures should be necessary, proportionate, evidence-based and as minimally intrusive as possible. Protecting children should not come at the expense of their other fundamental rights.

What specific challenges does AI present?

AI can amplify existing online risks and introduce new concerns, including harmful interactions with chatbots, emotional attachment to AI companions and automated decisions affecting children's welfare, education and healthcare. Child-rights impact assessments, safety standards and appropriate safeguards should be in place before products are deployed. Human accountability must remain central to decisions affecting children.

Why is international cooperation necessary?

Digital services operate across borders, while regulatory standards and enforcement capacities differ between countries. Inconsistent safeguards can leave children in some jurisdictions less protected than others. Regional and international cooperation can help align standards, strengthen accountability and increase governments' collective influence over technology companies.

3. STRATEGIC TAKEAWAYS FOR DIPLOMATS

Several practical priorities emerge for strengthening the protection of children's rights in the digital environment.

- **Move from principles to implementation.** Existing human rights standards provide an important foundation, but they need to be translated into national policies, legislation, institutional capacity and effective enforcement mechanisms. National frameworks should bring together digital policy, digital economy considerations, children's rights, child protection and support systems, with clear roles and responsibilities.

- **Adopt proportionate and evidence-based regulation.** Measures should respond to clearly identified harms and objectives rather than relying on blanket restrictions. Age assurance, content restrictions and other regulatory tools should be assessed for their effectiveness, proportionality, privacy implications and potential for circumvention.

- **Put safety into design.** Child safety should be integrated into the design and development of digital services and AI systems from the outset. Companies should assess potential impacts on children before products are deployed and apply appropriate safeguards across jurisdictions rather than limiting stronger protections to countries with more stringent regulation.

- **Strengthen accountability for companies.** Commercial incentives can influence how quickly and extensively safety measures are implemented. While voluntary frameworks remain relevant, enforceable legal obligations are an important mechanism for ensuring that companies design and operate products in ways that respect children's rights.

- **Build effective support and referral mechanisms.** Protection measures should be connected to systems through which children can safely report harm and access meaningful support. These mechanisms need to be trusted by children and linked to institutions capable of responding effectively.

- **Involve children and young people.** Children should not only be viewed as beneficiaries of protection measures. Their experiences, priorities and perspectives should inform the development of digital policies and regulatory frameworks. Regional approaches have increasingly incorporated child and youth participation as an important element of policy development.

- **Strengthen regional and international cooperation.** No State can address the challenges of the digital environment alone. Cooperation can facilitate the exchange of evidence, good practices and regulatory approaches, while supporting greater consistency in the protection afforded to children across borders. Current initiatives discussed included the Human Rights Council process led by Egypt, regional consultations, and the Global Coalition for Children's Rights and Protection in the Age of AI.

- **Preserve the opportunities offered by digital technologies.** Protection should not be understood solely in terms of restricting risks. Meaningful connectivity, digital education and access to information remain important opportunities for children, including in contexts affected by conflict and disruption to traditional education. Safety and opportunity should therefore be pursued together.

CONCLUSION

The central challenge in protecting children in the digital age is not simply technological innovation, but ensuring that governance, regulation and institutional capacity keep pace with it. Digital participation is already an integral part of children's lives and, increasingly, a condition for exercising other rights. The existing human rights framework provides a foundation, but implementation remains uneven and significant gaps persist. The policy challenge is how to make that participation safe, meaningful and rights-respecting.

A sustainable approach requires moving beyond isolated solutions and recognising that children's digital experiences are inseparable from their lives offline. Safety, privacy, participation, freedom of expression, access to information and dignity must be considered together, rather than treated as competing objectives. At the same time, responsibility must extend beyond children and families to governments, technology companies and other actors with the power to shape the digital environment.

National regulation remains an important starting point, but the cross-border nature of digital technologies makes regional and international cooperation increasingly necessary. Sharing evidence, strengthening common standards, coordinating regulatory approaches and ensuring meaningful participation by children and young people can help bridge implementation gaps.

Ultimately, the objective should be to create a digital environment in which children can participate meaningfully, access opportunities and exercise their rights while being protected from harm. As the discussion highlighted, safety and opportunity should go hand in hand.

As AI continues to develop at unprecedented speed, the central policy question is no longer whether regulation can keep pace with technology. It is whether governments, companies and international institutions are prepared to act early enough to ensure that children's rights remain at the centre of technological development.

GENEVA CENTRE FOR HUMAN RIGHTS ADVANCEMENT AND GLOBAL DIALOGUE

Rue de Vermont 37-39
CP 186 • 1211 Geneva 20
Switzerland

Phone: +41 22 593 22 50

Email: info@gchragd.org

Follow us

