



Global Digital Compact Consultation

Joint submission by 43 Child Rights Organisations

Under thematic area 4 “Apply Human Rights Online”

25 April 2023

#SafeOnline





Introduction

Together with five expert organizations (5 Rights Foundation, ECPAT International, International Telecommunication Union (ITU), WeProtect Global Alliance and World Childhood Foundation Sweden) the End Violence Partnership has prepared a joint submission to advocate for the protection of children from online risks and harms to be meaningfully integrated across the [Global Digital Compact](#). The consultation aims to inform the design of the Global Digital Compact that will outline ‘shared principles for an open, free and secure digital future for all’ to be agreed at the Summit of the Future in September 2024.

We need to make sure children’s rights to protection online are taken into account in the global digital agenda. This joint submission brings together the expertise and voices of 43 child rights organizations and partners to outline critical principles and commitments key actors should follow to ensure the digital world is safe for children.

Core principles that all governments, companies, civil society organisations and other stakeholders should adhere to:

The implementation of children’s rights online along with the digital safety of children needs to be at the forefront of the Global Digital Compact across all its components. Digital technologies have created exceptional opportunities to advance the human condition including opportunities for children but have also created spaces for abuses at an unprecedented scale and with an increasingly profound impact on the health, wellbeing and future prospects of children of all ages and backgrounds. The rapid expansion of information and communication technology has created exceptional opportunities for children and young people to know their rights and access information as more and more children are connecting for the first time every day, either on personal or shared devices. However, wider and more easily available access to the Internet and digital technology also poses significant challenges to meaningful connectivity and children’s rights, including their safety. Impacts range from threats to protection of personal data and privacy, to harassment and cyberbullying, harmful online content, grooming for sexual purposes, and sexual abuse and exploitation.

One of the worst unforeseen consequences of the rise of the internet and digital technologies has been the exponential growth in online child sexual exploitation and abuse (CSEA) which comes in many forms and includes grooming, live streaming, consuming child sexual abuse material, and coercing and blackmailing children for sexual purposes. Online CSEA can be interconnected with other forms of violence like gender-based violence, stalking, bullying, cyber-aggression and cyber-harassment and trafficking. It violates children’s fundamental rights and may result in long-term harm for victims and survivors.

The latest data shows that 15% of children reported cyberbullying victimization, and 11% of 9–16-year-old across 19 European countries had experienced misuse of their personal information or password, or theft of their digital identity. In the past year, fewer than 40% of children had come across websites where people talked about or displayed gory or violent images or had seen images of a sexual nature, and less than one quarter of children in surveyed countries said that they had seen online content related to physical self-harm ([Annual report to the Human Rights Council](#) of the Special Representative of the Secretary General on Violence against Children, January 2023).

The prevalence of online CSEA has already been highlighted as a “major concern” in the 2020 UN roadmap for digital cooperation. In the last two years this crime has continued to grow at exponential rates. In 2021, the [National Center for Missing & Exploited Children](#) received 29.3 million reports of suspected child sexual exploitation (an increase of 35% from 2020). The multi-country research project [Disrupting Harm](#) shows that up to 20% of 12–17-year-olds across 13 countries were subjected to online CSEA in the past year alone; scaled to the general population of internet-using children, these estimates represent millions of children in each country. A scarcity of data remains on this crime, but available data shows that: victims of online CSEA





fall into all age groups, but they are increasingly getting younger; while girls seem to be more affected, for boys the abuse may be more severe; perpetrators are more likely to be someone the child already knows in person; online violence is often associated with experiences of in-person violence; and, it has devastating impact on children's physical and mental health.

The Global Digital Compact should unite and lead the world to reverse this wave of online sexual abuse of children via applying children's rights frameworks online and to frontier issues and new technologies. The [UNCRC General Comment 25](#) adopted in March 2021, formally established children as rights holders in the digital environment, and noted that "States parties should take legislative and administrative measures to protect children from violence in the digital environment, including the regular review, updating and enforcement of robust legislative, regulatory and institutional frameworks that protect children from recognized and emerging risks of all forms of violence in the digital environment." The World Economic Forum Global Principles on Digital Safety ([White paper](#), January 2023) highlights the need for (1) collaboration across stakeholders; (2) inclusive and informed decision-making; (3) evidence-based and innovative solutions to prevent risks and harms in digital environments; (4) transparency across all actors; (5) realization of digital rights of vulnerable and marginalized groups, including protecting children's safety and privacy. Industry actors have also made some progress to create shared frameworks and principles to tackle this crime and better define their role. For example, in 2020 the Five Country Ministerial launched the [Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse](#) created in partnership with leading tech companies and WeProtect Global Alliance, and in 2022 the Tech Coalition launched the [Voluntary Framework for Industry Transparency](#), led by industry partners following a consultation process with civil society and Governments. Such processes showed the importance of acknowledging the diversity of the digital technology industry, that voluntary action is not enough, and that more proactive measures for ensuring transparency and accountability of industry approaches to child safety online are needed.

The principles along with what is needed to apply them to shape a safe and trusted digital world for children are clear, and the Global Digital Compact is the vehicle to make this happen.

Key commitments, pledges, or actions that in your view should be taken by different stakeholders – governments, private sector, civil society, etc. - in order to realize the above-mentioned principles.

To translate the above principle into practice and meaningful, global change, key stakeholders, especially governments and private sector, need to take **several steps** individually and jointly, aligned around the same goal to create digital spaces where children can be safe and thrive.

The [UN Roadmap for Digital Cooperation](#) already outlined some **key commitments needed**: *important legislative steps, effective cooperation* (especially between law enforcement agencies and technology companies including more robust, rapid scanning and detection with a great focus on prevention), and *continued investment in multi-stakeholder partnerships* (e.g. WeProtect Global Alliance and End Violence Partnership). In addition to these, a group of leading experts convened by the End Violence Partnership identified **three core commitments for Governments and private sector** based on evidence, research and expertise on what works to protect children ([Safe Online Policy Call](#)):

- Ensure an aligned and coordinated national and industry response via the *adoption and implementation of comprehensive child online safety policies* based on a child's right to access the digital world safely and securely. These policies should be in-line with the UNCRC General Comment 25 on children's rights in the digital environment.
- Commit to preventing, detecting and stopping all activities that harm children online by *applying existing frameworks*. For example, the recommendations outlined in the ITU Guidelines on Child Online Protection for policymakers, ICT Industry, caretakers, educators and children; the WeProtect Global Alliance





Model National Response (MNR) and **Global Strategic Response (GSR)** to support governments, private sector, international organizations and civil society to better protect children from online CSEA which is already used by the Alliance members (90% of **42 surveyed countries** confirmed they have used the MNR to understand and develop good practice at the national level); and, the *six actions* outlined by the **Broadband Commission Report** to build key capacities and capabilities needed to tackle online CSEA and to continue learning through their implementation across the world.

- Increase *investments to scale-up solutions* that keep children safe, particularly those that tackle grooming, live streaming and distribution of CSAM, to address the imbalances in capacity across countries and enable effective international collaboration and response.

In the addition to the above core commitments, key stakeholders need to **commit and allocate adequate resources** to ensure the following:

- All efforts to expand connectivity and digital education must go hand-in-hand with child safety.
- Ensure a universal response where everyone plays a role with a focus on primary prevention, and safety-by-design.
- Technology tools to tackle online violence against children should be a public good while acknowledging the need for more controlled access to certain types of tools for processing sensitive information, and technology companies must be at the forefront of the response and promote responsible innovation.
- Promote industry transparency and create stronger mechanisms for coordination and accountability for effective response on reporting to industry and quality support services.
- In line with the **UNCRC General Comment 25**, legislations should be in place and be implemented to ensure business responsibility and accountability for the respect of children's rights in digital environments, notably by carrying out child rights risk assessments and ensuring a high level of privacy, safety and security by design and default.
- Generate data and evidence to inform and drive prevention and response to online violence against children and especially the worst forms such as online CSEA. Investments should address all forms of online violence against children in an integrated way, both across types of violence and alongside its in-person forms.
- Listen to children and increase public awareness of online CSEA; messaging should be developed in meaningful consultation with children and backed by evidence.
- Safety and protective measures should be designed and implemented in accordance with children's evolving capacities depending on their age and abilities.
- Where children have carried out online harm, governments should pursue preventive, safeguarding and restorative justice approaches for the children involved.

Tools already exist to guide and assist actors to make this happen – e.g. **ITU Child Online Protection Guidelines**, **Child Online Safety Toolkit**, **Legislating for the digital age**, **eSafety Self-assessment Tools for Technology Companies**, **UNICEF Child Rights Impact Self-Assessment Tool for mobile operators**, **UNICEF & Western Sydney University Responsible Innovation in Technology for Children**. The above actions and commitments will ensure an aligned and coordinated response across stakeholders, create the very much needed key capacities and capabilities that are needed to tackle online sexual abuse, and address the imbalances in capacity across countries and enable effective international collaboration and response.





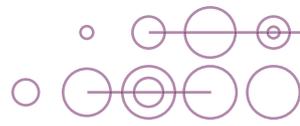
Developed by

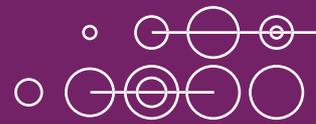


Endorsed by

- Aulas en Paz Colombia
- Child Rescue Coalition
- ChildFund Alliance
- Childlight - Global Child Safety Institute
- Childline Zimbabwe
- ChildSafe Net Nepal
- Corporación Colombiana de Padres y Madres Red PaPaz
- Family Wellbeing Centre Sri Lanka
- Fundacion Paniamor Costa Rica
- Huddersfield University
- International Justice Mission
- International Safety Center Stop Sexting Ukraine
- Internet Hotline Provider Macedonia
- Internet Watch Foundation
- itotheN
- Justice and Care
- Marie Collins Foundation
- Middlesex University
- Missing Children Europe
- MSB Medical School Berlin
- New Hope Girls NHG République Démocratique du Congo
- Oficina de Defensoria de Derechos de la Infancia Mexico
- Pathfinder Kindred Ltd
- Population Foundation of India
- SaferNet Brazil
- Save the Children International
- Shanduko Yeupenyu Child Care Zimbabwe
- Suojellaan Lapsia Protect Children Finland
- Swansea University
- Tech Matters
- Terre des Hommes International Federation
- Thorn
- University of Kent
- Universidad de los Andes Colombia
- World Vision International
- Youth Association for Development Pakistan
- Zana Africa Foundation Kenya







Every child must be **#SafeOnline!**

To know more, contact
secretariat@end-violence.org



Learn more about
Safe Online [here](#)

