# G7 Common Set of Principles defining a safer and more secure digital space for minors

**1. We, the G7 Digital and Technology Ministers, are committed to working in favor of a safer and more secure digital space for minors, which includes children and adolescents. In order to safeguard their physical, mental, and cognitive well-being and development, future-proof principles are needed to guide our ongoing responses to protect minors against a wide range of risks, digital services commitment to online safety, and our mutual goals to safeguard safety, privacy, freedom of expression online, human rights and fundamental freedoms. These principles will contribute to empowering parents, families, guardians, healthcare professionals and teachers, so that minors can benefit fully from new technologies and safe online experiences.**

**2. Digital services can be a powerful tool to learn, discover and exchange. Besides, digital literacy and AI education for minors, guardians, and teachers can contribute to help minors to engage confidently in the digital world and benefit from it**. Still, concerns have been raised regarding risks, including from the scientific community, for minors of excessive screen time and the use of certain digital services that incorporate attention and engagement maximizing features, threaten their physical and mental health, as well as their privacy, security, well-being, and cognitive and social development. These can lead to compulsive, habit-forming, and other problematic uses and behaviours, which may impact self-esteem and further threaten their health.

**Without shared efforts and comprehensive approaches to foster online safety by digital services providers, governments and guardians, minors can also be exposed to illegal and age-inappropriate content and interactions across digital services, damaging their mental health and well-being**. This notably includes exposure to online harassment, grooming, self-harm, recruitment by organized criminal groups, criminal activities, unwanted or illicit sexual solicitations, and to child sexual exploitation and abuse (CSEA), and criminal activity relating to non-consensual intimate imagery (NCIIs).

**New technologies such as generative AI, notably chatbots, while bearing benefits, can replicate or exacerbate existing risks for minors while taking new forms**. Particular concern exists regarding non-consensual intimate imagery, AI-generated child sexual abuse material, sexually exploitative or pornographic content, and deceptive, violent, or coercive interactions and content – such as deepfakes and manipulative simulated interactions. Such risks, which undermine minors' well-being and safety, reinforce the need for minors to be able to distinguish synthetic content, to identify content provenance, and to build their critical digital skills to engage responsibly in digital spaces. As these technologies continue to evolve and proliferate, people need support to develop digital literacy to ensure they can engage critically and responsibly in digital spaces. Principles are also needed to guide governmental response to better protect minors in vulnerable situations against aforementioned risks and to strengthen continued collaboration among stakeholders.

**3. We, G7 Digital and Tech Ministers, are committed to affirming the following principles defining a safer and more secure digital space for minors.**

**<u>Principle 1:</u> Effective age assurance is key to ensure a safer, more secure, and age-appropriate experience for minors.** Relying on robust, reliable, risk-based, appropriate, rights-respecting, privacy-preserving and interoperable age assurance solutions, this principle should be implemented as a step to facilitate an age-appropriate digital experience for minors and to prevent them from being exposed to digital services or products that are illegal for them, such as pornography, alcohol or tobacco, and for digital services that pose risks for minors, consistent with applicable laws. Because protecting freedom of expression and privacy is a core part of protecting minors online and fundamental to free societies, age assurance should be applied in ways that allow for, when needed, parental consent, and compliance with applicable legal obligations through the least invasive means, that are appropriate, privacy-preserving, fair and technically feasible.

**Principle 2: Protect minors from harms online through safety by design approaches such as protective and by default settings, including parental control tools, which prevent minors from being exposed to content, interactions and features that are not age appropriate, safe and secure.** Minors' accounts privacy and safety should be ensured through default settings, as well as by providing parents tools to manage their children's default privacy and safety settings, helping minors and parents to limit their screen time and to prevent minors from specific risks such as being geolocated or contacted without consent, and from functionalities leading to compulsive or habit-forming use. Furthermore, governments should collaborate with the private sector, civil society and researchers to informing discussions on these parameters.

**In particular, it is key for minors that recommendation systems, when used, are designed to elevate age appropriate content and reduce exposure to risks.** They should not maximize minors' attention and engagement online, but rather give parents and minors setting tools to be more in control of their experiences and data online.

**Principle 3: The creation and distribution of child sexual abuse material and criminal activity related to non-consensual intimate imagery must be prevented, consistent with G7 members' current applicable legal obligations.** The creation, possession and distribution of child sexual abuse material is illegal across G7 countries and urgent action needs to be taken to prevent the ongoing circulation of material across the globe and support the rights of victims and survivors. This includes responding to AI-generated CSAM and NCII. This builds upon priority action in the voluntary G7 Action plan to combat child sexual exploitation and abuse (2021) where industry is encouraged to at a minimum endorse the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (2020) which sets out a baseline set of voluntary actions that companies can implement to address the scale and nature of this harm. The sharing and continued circulation of non-consensual intimate imagery, including AI-generated NCII, also further amplifies the need for concrete preventative action. As this type of abuse can have prolonged trauma for victims, it is important to ensure that victims and survivors have help and support available to them, and that law enforcement authorities are equipped when conducting investigations.

**Principle 4: Parents, guardians and carers should be equipped with easy-to-use, privacy-respecting, effective parental control tools that are interoperable when technically feasible to help guide and empower minors online**. Robust tools help parents and guardians to manage their children's privacy settings and screen time and, content exposure and account controls. Digital services providers and governments should propose awareness and education campaigns to support digital literacy, digital tools, and empower families to effectively navigate and harness the benefits of digital environments. These complementary tools should be effective and compliant with applicable legal frameworks and rights, and can be developed in cooperation with healthcare professionals and educational systems and other relevant actors.

**Principle 5: Minors should be empowered with a comprehensive education focused on building the necessary literacy and skills in order to better understand digital systems, and critically engage with digital technologies, media and information, to recognize risks and thrive online.** In addition, digital services providers should promote accessible tools, parameters and features, and effective screen time management tools for both parents and minors. These should improve user data transparency, create an awareness of how data is used to personalize or influence shape their experience and provide clear options for modifying settings, so that they can make informed independent decisions regarding the use of these systems. Besides, this principle can be supported by promoting AI literacy and by ensuring that users, especially minors, are able to seamlessly identify synthetic content and its provenance through technical means.

While progress has been made, digital services should continue innovating to strengthen the protection of minors in digital spaces. This includes developing terms and conditions that are clear and accessible for minors, conducting awareness-raising efforts that use age-appropriate language to explain potential risks associated with different technologies, providing tools for digital skill building, proposing mitigation strategies, and prominently displaying easy to find mechanisms where minors, parents, and guardians can report harms and illegal content.

**<u>Principle 6:</u> Minors' safety is ensured safeguarded by the implementation of risk management, assessment and mitigation, and following safety-by-design approaches.** Consistent with G7 members' current applicable legal obligations, digital services should maintain responsive efforts to assess and mitigate the wide range of risks and adapt their protection frameworks including for example specific risk-mitigation measures, rapid alert systems, such as for criminal activities, signposted support resources, and minors-friendly reporting mechanisms. In order to preserve innovation from being outshone by risks, digital services providers should promote meaningful transparency regarding relevant practices and safeguards throughout the design and development of products and services, notably regarding minors' and parents' human rights and fundamental freedoms, ensuring that they are age-appropriate and support minors' safety, autonomy and healthy development. Finally, they are needed to support evidence-based approach of minors' safety.

**<u>Principle 7:</u> Building a safer and more secure digital space for minors is enabled by digital service providers' cooperation with relevant stakeholders.** This close cooperation and dialogue between governments and stakeholders, including consulting and working with researchers, parents, guardians, teachers, healthcare professionals, civil society, companies, minors' development experts, academics, and, when applicable, public authorities, is essential to address aforementioned risks online, and to get a better understanding of the relevant risks. In order to support an evidence-based approach, transparency and accountability are essential, as well as impartial assessment and evaluation of risks. Enabling data sharing with relevant stakeholders and fostering evidence-based approaches can improve understanding of the relevant risks. A shared evidence base will increase the relevance of research in this domain and strengthen the solutions available to protect minors online.

**4. We, G7 Digital and Technology Ministers, support these principles. For this purpose, while noting that different jurisdictions may take their own unique approaches to implementing these guiding principles:**

- We call on digital services providers to translate these principles into actions, and to closely cooperate with all relevant stakeholders to determine practical ways of implementing these principles.

- We affirm that an evidence-based approach includes actively listening to the voices of minors, parents and guardians in the development of public policies that concern them, and to ensuring the protection of minors' rights in the digital environment.

- We are committed to fostering synergies and international cooperation between G7 partners and relevant actors, and to further enhancing cooperation between our governments, with a view to applying the necessary, rights-respecting measures consistent with the principles and defining common priority research areas to better characterize and mitigate aforementioned risks.