



G7 Digital and Technology Track - Annex 3

G7 INTERNET SAFETY PRINCIPLES

The COVID-19 pandemic has driven a steep increase in the use of the internet and different services provided online, such as social media, and has clearly demonstrated the importance of improving internet safety. Online content that is illegal, and content that is harmful, can have a major impact on people, especially women and children, and on our societies. In the principles set out below:

- The G7 **RECOGNISES** that international cooperation is vital to address the shared global challenge of internet safety. This cooperation should be multi-stakeholder in nature and include governments, companies, academia, civil society and other interested stakeholders.
- We **RECOGNISE** and seek to complement the important work in existing fora towards enhancing a safe online environment, including the Christchurch Call to Action, the upcoming OECD Recommendation on the Protection of Children in the Digital Environment, the G7 Rapid Response Mechanism, the work of the Global Internet Forum to Counter Terrorism, the WeProtect Global Alliance, the Technology Coalition Fighting Child Sexual Abuse, and current and previous G7 initiatives.

Underpinning Principles

1. Fostering Human Rights Online

- We **COMMIT** to promoting and protecting the exercise of all human rights online, including, but not limited to, freedom of opinion and expression (including the right to seek, receive or impart information), as well as the right to privacy as set out in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights; and we will help more people to enjoy their right to freedom of expression by enabling them to participate in online activities and engage in robust debate online.



2. Multi-Stakeholder Approach

- We will **CONTINUE** our support for a multi-stakeholder approach to policy-making, working with companies, civil society, academics and representative groups, in particular those who are especially impacted (including, but not limited to, women, the elderly, persons with disabilities, children, minority ethnic and religious groups), to reflect their experiences and voices in decision-making about improving internet safety and reducing harmful online content and activity.

3. Corporate Responsibility

- We **BELIEVE** that, including as part of their corporate social responsibility, companies should have the systems and processes in place, including safety by design principles, to take appropriate action with relevant stakeholders, including civil society and academia, to improve internet safety and reduce illegal and harmful content and activity in the online environments that they create, while respecting human rights online.

4. Transparency and Accountability

- We **BELIEVE** that companies should be transparent, including with consumers, about the presence of known illegal and harmful activity on their services, and the decisions and measures taken to improve internet safety, as well as be accountable for the decisions made to counter illegal and harmful content in line with their terms and conditions at global, national, and regional levels.

Operational Principles

5. Research and Best Practice in Safety Technology

- We **COMMIT** to sharing information, research and best practice for the development and adoption of safety technology, and to supporting innovation that drives digital growth and **URGE** providers of consumer services online to ground their internet safety policies and practices in research and evidence.



6. Protecting Children

- We **BELIEVE** that companies designing, providing or using services for children, or online spaces that may be used by children, should prioritise the protection of children on their services and provide safety measures to ensure children are protected from both illegal and harmful content and activity, in line with the upcoming OECD Recommendation on the Protection of Children in the Digital Environment.

7. Online Media Literacy

- We **BELIEVE** that governments, companies, civil society, academia and other interested stakeholders need to educate and empower people of all ages with the skills, digital competence, access and knowledge they need to make informed and safe choices online; and evaluate and develop domestic approaches to keep pace with new technologies and their applications.

8. Youth Participation

- We **BELIEVE** young people can be active agents for change and we have the responsibility to empower young people to shape conversations and play a positive and active role in promoting and improving internet safety.