

OFFICIAL: Sensitive

Commissioner briefing – WEF Global Principles on Digital Safety launch

To:	Julie Inman Grant (Commissioner)
From:	International Strategy and Futures branch
Date:	12 January 2023
Subject:	Upcoming event at Davos to launch WEF's digital safety principles
Meeting dates, times	Global Coalition for Digital Safety: Tuesday 17 Jan 15:30 – 16:30 CET Tackling Harm in the Digital Era: Wednesday 18 Jan 17:30 – 18:15 CET

Purpose

The Global Principles for Digital Safety will be launched at Davos 2023. There are two meetings that will support the launch:

- A meeting of the Global Coalition for Digital Safety to showcase the principles and broader work of the group
- A panel session on tackling harm to discuss regulatory, industry and societal efforts and innovations undertaken by all stakeholders in the digital ecosystem to advance digital safety (nb. Marketing and Communications will provide talking points for this session).

Recent engagements

- Representatives from eSafety have engaged with WEF representatives through regular working group meetings for the WEF Coalition for Digital Safety.:
 - Workstream 1 – Global charter of principles for digital safety. We are not a working group member but responded to specific questions to inform the development of the principles, provided feedback on their first draft and contributed to a roundtable session which finalised the first issue. The principles were [soft-launched](#) 9 Jan.
 - Workstream 2 – Toolkit for digital safety design interventions and innovations. We're co-chairing this workstream with Crisp Thinking and are on track to deliver:
 - Typology of online harms – March 2023
 - We're collaborating with Crisp on a first version of the typology, incorporating feedback provided by the working group around the in-person roundtable held 16 Nov 2022, and will share for EM and Commissioner review 8 Feb
 - We aim to share the typology with the working 20 Feb, giving them two weeks to provide feedback

OFFICIAL: Sensitive

OFFICIAL: Sensitive

- The intention is to hold another in-person roundtable to finalise the typology of harms and introduce the vectors for weaponization product in New York w/c 6 March (to be confirmed with Commissioner's office)
- Final comments / thoughts will be incorporated into the typology for publication at the end of March (exact date TBC).
- Vectors for weaponization product – June 2023
- Typology of future online harms – Q3 2023
- Interventions product – Q3 2023
- Workstream 3 – Digital safety risk assessment framework. The following workstream objectives have been agreed:
 - Bank of Case Studies: collection of case studies illustrating best/good/poor practices that can be leveraged to tease out the interconnectedness and trade-offs across human rights (Feb 23)
 - Report clarifying risk factors that should be used to identify digital safety risks (May 2023);
 - Recommendations on good/best practices to support companies steering toward more effective digital risk assessment (Sept. 2023)
- We're a working group member and assigned as a contributor, alongside Inbal Goldberger (ActiveFence) and Katherine Sandel (Google), to a Safety by Design case study. Julia Fossi (AWS), Matthew Soeth (Spectrum Labs), Eliska Pirkova (Access Now), Benoit Loutrel (Arcom) and Lee Huan Ting (IMDA) are assigned as reviewers (Nb. this list has been updated per WEF correspondence of 9 Jan).
- In the most recent working group meeting we discussed using a conceptual case study of a product / service aimed primarily at children and running it through a SbD assessment tool. We will report on aspects such as assessment metrics, contributing regulatory obligations, benefits / risks and resource requirements in the case study template

Background

Global Principles for Digital Safety

- The workstream has attempted to answer the fundamental question:
 - *How do international human rights principles translate in a digital context?*
- The principles aim to advance digital safety in a rights-respecting way, drive multistakeholder alignment, encourage positive behaviours and actions across the digital ecosystem, and inform and enable regulatory, industry and societal efforts and innovations.
- The Working Group includes representatives from Microsoft, WeProtect Global Alliance, Meta, Amazon, Google, OHCHR (UN Office of the High Commissioner for Human Rights), Ofcom UK, Global Partners Digital.
- To summarise, the principles include:
 - All supporters should collaborate to build a safe, trusted and inclusive online environment. Policy and decision-making should be made based on evidence, insights and diverse perspectives. Transparency is important, and innovation should be fostered.
 - Supportive governments should distinguish between illegal content and content that is lawful but may be harmful and differentiate any regulatory measures accordingly, ensure

OFFICIAL: Sensitive

OFFICIAL: Sensitive

law and policy respect and protect all user rights. They should support victims and survivors of abuse or harm.

- Supportive online service providers should commit to respecting human rights responsibilities and devise policies to ensure they do, ensure safety is a priority throughout the business and that it's incorporated as standard when designing features (Safety by Design), and collaborate with other online service providers.
- The principles are available for [download](#) on the WEF website and are included as an attachment to this briefing.

Digital Human Rights

Under the Online Safety Act (s 24), the eSafety Commissioner must, as appropriate, have regard to the UN Convention on the Rights of the Child in the performance of its functions.

Industry should do the same in accordance with the [Children's Rights and Business Principles](#) developed by UNICEF, the UN Global Compact and Save the Children.

Relevant right under the UNCRC	Commentary
Article 2: Non discrimination	States should ensure that all children have equal and effective access to the digital environment in ways that are meaningful for them. This includes providing safe access. Children may be discriminated against by their being excluded from using digital technologies and services or by receiving hateful communications or unfair treatment through use of those technologies. Discrimination can often be intersectional, with age-based discrimination being compounded by sexism, racism, ablism, etc (examples: PVARO work)
Article 3: best interests of the child	The best interests of the child should be the primary consideration in designing and governing the online environments they inhabit (examples: Safety by Design approach)
Article 5: parental guidance and a child's evolving capacities	Online safety efforts should engage parents and carers and support them to provide guidance to children in accordance with their evolving capacities (examples: our resources for parents)
Article 12: respect for the views of the child	Children should be consulted on their views and have their views taken into account in designing and governing the digital world (examples: youth engagement research, YAC, SbD youth vision statement)
Articles 13, 14, 15 and 17: freedom of expression, thought, association and access to information	Children have a right to express themselves online, as well as the freedom to seek, receive and impart information and ideas of all kinds, using any media of their choice. Restrictions on children's right to freedom of expression in the digital environment, such

OFFICIAL: Sensitive

	as filters, including safety measures, should be lawful, necessary and proportionate.
Article 16: right to privacy	Privacy is vital to children’s agency, dignity and safety and for the exercise of their rights. This means ensuring that appropriate measures are in place where children’s data may be processed. Data may include information about children’s identities, activities, location, communication, emotions, health and relationships.
Articles 19, 34 and 36: protection from violence, abuse and neglect; sexual and other forms of exploitation	All appropriate measures should be taken to protect children from risks to their right to life, survival and development. Risks relating to content, contact, conduct and contract encompass include violent and sexual content, cyberbullying and harassment, exploitation and abuse, including sexual exploitation and abuse, and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist. Children should have access to help and support to prevent and mitigate these harms (example: our complaints schemes)
Article 28: right to education	It is of increasing importance that children gain an understanding of the digital environment, including its infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance, and of the possible negative effects of digitalization on societies (example: our education resources)
Article 37d: right to remedy	There should be efforts to ensure that appropriate and effective remedial judicial and nonjudicial mechanisms for the violations of children’s rights relating to the digital environment are widely known and readily available to all children and their representatives. (e.g. regulation). (example: our complaints schemes)

General background on human rights in the digital environment

Human rights are often described as inalienable and universal, however there is global recognition of the possibility for tension between rights in practice, which can allow for de facto limitations on a person’s ability to exercise specific rights.

In such cases, governments might be justified in restricting one right to ensure the enjoyment of another. However, such restrictions should be necessary, proportionate, and “determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of

OFFICIAL: Sensitive

others and of meeting the just requirements of morality, public order and the general welfare in a democratic society”¹.

There is a growing body of scholarship in interest in considering the impact of digital transformation on the interplay and tensions between rights. This includes work from the UN Council on the Rights of the Child General Comment 25 on children’s rights in relation to the digital environment², and the Organisation for Economic Co-operation and Development (OECD), which has recently published a report into Rights in the Digital Age³.

The rights to privacy and freedom of expression have been given more attention in the early development of the digital environment. However, the rapid expansion of access to digital spaces for people of all ages, backgrounds, locations and levels of experience with technologies and the shift towards the digitisation of people’s everyday activities have made the right to safety increasingly important. The right to safety is implicit throughout the core international human rights treaties, but are clearest in the following articles:

- Article 3 of the Universal Declaration of Human Rights:
‘Everyone has the right to life, liberty and security of person’
- Article 20(2) of the International Covenant on Civil and Political Rights (ICCPR):
‘Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.’
- Article 19(1) of the Convention on the Rights of the Child
‘States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child’
- Article 16 (1) of the Convention on the Rights of Persons with Disabilities:
‘States Parties shall take all appropriate legislative, administrative, social, educational and other measures to protect persons with disabilities, both within and outside the home, from all forms of exploitation, violence and abuse, including their gender-based aspects.’
- Article 12 (1) of the International Covenant on Economic, Social and Cultural Rights
‘The States Parties to the present Covenant recognize the right of everyone to the enjoyment of the highest attainable standard of physical and mental health.’
- The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) and the International Convention on the Elimination of All Forms of Racial Discrimination

¹ Universal Declaration of Human Rights, Article 29,
https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf

² Committee on the Rights of the Child (2021), General Comment no. 25 on Children’s Rights in Relation to the Digital Environment, <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

³ Organisation for Economic Cooperation and Development (2022), Rights in the digital age – Challenges and Ways Forward of the United Nations High Commissioner for Human Rights (2022), What are human rights?, https://www.oecd-ilibrary.org/science-and-technology/rights-in-the-digital-age_deb707a8-en

OFFICIAL: Sensitive

(ICERD) also recognise rights to equality and non-discrimination, which can include protections against violations of the right to safety.

OFFICIAL: Sensitive

Appendix

Current list of meeting attendees for Tackling Harms in the Digital Era panel session:

Status	Name	Position	Organization
Confirmed	Jean-Noël Barrot	Minister-Delegate for the Digital Transition and Telecommunications	Ministry of Economy, Finance and Industrial and Digital Sovereignty
	Petra De Sutter	Deputy Prime Minister and Minister of Public Enterprises, Public Administration, Telecommunications and Postal Services of Belgium	Office of the Prime Minister of Belgium
	Egils Levits	President of Latvia	Chancery of the President of Latvia
	Melanie Dawes	Chief Executive	Office of Communications (Ofcom)
	Julie Inman Grant	eSafety Commissioner	Office of the eSafety Commissioner
	Jürgen Stock	Secretary-General	International Criminal Police Organization (INTERPOL)
	Shou Zi Chew	Chief Executive Officer	TikTok
	Monika Bickert	Vice-President, Content Policy	Meta Platforms Inc.
	Kent Walker	President, Global Affairs	Google
	Nadav Shoval	Chief Executive Officer and Co-Founder	Open Web Technologies Ltd.
	Dorit Dor	Chief Product and Technology Officer	Check Point Software Technologies Ltd
	Noam Schwartz	Chief Executive Officer and Co-Founder	Activefence Ltd. (515838092)
	Tirana Hassan	Acting Executive Director	Human Rights Watch
	Brett Solomon	Co-Founder and Executive Director	Access Now
	Lauren Woodman	Chief Executive Officer	DataKind
	Nighat Dad	Founder and Executive Director	Digital Rights Foundation
	Eileen Donahoe	Executive Director	Global Digital Policy Incubator

OFFICIAL: Sensitive

OFFICIAL: Sensitive

	Heidi Larson	Professor of Anthropology, Risk and Decision Science	London School of Hygiene and Tropical Medicine
	Hoda Al Khzaimi	Assistant Research Professor, Engineering Department	New York University - Abu Dhabi
Invited	Josephine Teo	Minister for Communications and Information	Ministry of Communications and Information (MCI) of Singapore
	Vera Jourovà	Vice-President for Value and Transparency	European Commission
	Koh Jean	Chairman	Presidential Committee of Digital Platform Government, Korea
	Mykhailo Fedorov	Vice-Prime Minister, Minister of Digital Transformation	Ministry of Digital Transformation of Ukraine
	Paula Ingabire	Minister of Information Communication Technology and Innovation	Ministry of Information Communication Technology and Innovation Rwanda
	Timo Harakka	Minister of Transport and Communications	Ministry of Transport and Communications of Finland
	Almar Latour	Chief Executive Officer, Publisher, Wall Street Journal	Dow Jones & Company Inc.
	André Kudelski	Chairman of the Board and Chief Executive Officer	Kudelski Group
	Jonathan Auerbach	Executive Vice-President; Chief Strategy, Growth and Data Officer	PayPal
	Michael Punke	Vice-President, Global Public Policy	Amazon Web Services

OFFICIAL: Sensitive