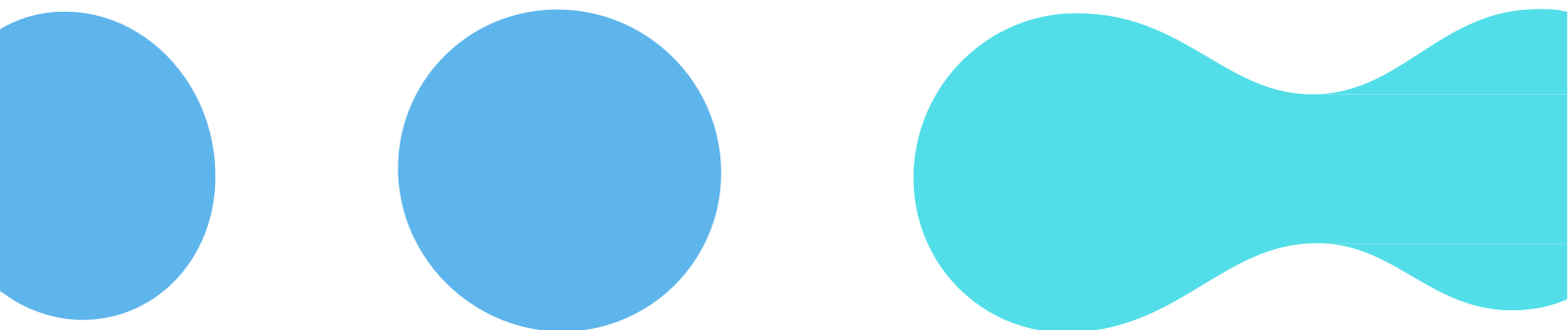




Global
Online Safety Regulators
Network

Position Statement

Regulatory coherence and
coordination: the role of the
Global Online Safety
Regulators Network



Introduction

The Global Online Safety Regulators Network ('the Network') was launched in November 2022 and is the first dedicated forum for independent online safety regulators around the world. The Network enables regulators to share experience, expertise, and evidence, paving the way for coherent international approaches to online safety regulation.

This statement articulates the Network's shared commitment to regulatory coherence and coordination – why we are prioritising it and the opportunity costs of not doing so. It outlines the policy areas where we will focus on and the levers that we will use to guide us in this work. Initially, our focus will be on developing common language and tools and on sharing regulatory insights, as well as issuing public statements on key global policy issues where the regulator's perspective would be additive to the international discourse.

Why we are prioritising coherence

First, though each of us has our own domestic regulatory framework, we understand that neither the risks people face online, nor the online services they use, are confined to national or continental borders. Accordingly, it is important that our regulatory approaches acknowledge this. With global service providers now being required to comply with online safety legislation in multiple jurisdictions, the possibility of cross-border regulatory fragmentation is heightened, potentially creating compliance challenges and costs for companies. By pursuing regulatory coherence, we can ensure that the online safety of internet users in our respective countries does not stop 'at the border' and that companies can benefit from compliance economies of scale and legal certainty.

Second, regulating a global industry that has accrued significant scale, power and resources brings challenges for individual countries. Through international regulatory coordination, we can exercise collective influence to achieve the safety outcomes set out in our respective online safety rules.

Third, each of us is grappling with challenging policy questions and establishing regulatory practices for a sector that itself is continually changing, both technologically and commercially. The regulatory tools we are applying (e.g., risk assessments, safety mitigations) are novel, as are the business models and technologies that we are applying them to. By working together on developing our regulatory capability and approaches, we

have a better chance of keeping abreast of important developments and implementing our respective regimes effectively.

Ultimately, the Network affirms its position that regulatory coherence and coordination will support an open, accessible, and safer digital ecosystem, which protects users from online harms and safeguards fundamental human rights.

Finding areas of commonality amid global diversity

The Network comprises a diverse range of regulators, each working under statutory remits borne out of different regulatory and legal traditions, and within different political and cultural contexts and norms. Despite these differences, our respective frameworks and regulatory mandates are similar in several key respects. Our approach will be to use the coordinating power of the Network to drive greater coherence in regulatory approaches across areas of similarity, and share learnings with each other where there are areas of difference.

For instance, our online safety rules are similar in their intended outcomes. We each aim to prevent and respond to online harms that impact individuals and communities. These can occur through the use of digital platforms by bad actors, or through product or service design choices by companies that are not made with safety by design or human rights principles in mind.

There is also a degree of commonality across the types of regulatory tools that we use (e.g., complaints mechanisms, transparency reporting, codes of conduct, risk assessments); the kinds of information that inform our work (e.g., metrics that measure harms trends or the impact of safety measures, complaints data, academic literature); and the regulatory approaches we take (e.g., sustained engagement with regulated services, consultation).

Moreover, each regulator's activity is underpinned by a demonstrated commitment to upholding human rights, democracy, and the rule of law, as well as political and commercial independence.

However, our respective rules differ in some ways, which can be seen in the table below. Here, the Network can offer learnings over time on the results yielded by different approaches, with an aim to inform future policy development.

The following table illustrates some of the similarities and differences in the regulatory remits of current Network members:

Regulatory remits and functions													
Jurisdiction	Ex ante regulation	User complaints and investigations					Information gathering and enforcement			Prevention research and engagement			
	Develop and enforce codes, standards, and guidance	Proactive content scanning	Receive and investigate individual user complaints	Issue content removal and blocking notices	Partnership with law enforcement and hotline networks	Service blocking or restriction orders (e.g., service, access, or payment blocking orders)	Oversight and transparency	Non-compliance notices and financial penalties	Court orders and injunctions	Education and awareness raising	Grants	Research and horizon scanning	Industry engagement
Australia (eSafety)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fiji (OSC)	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✓
France (Arcom)	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓
Ireland (An Coimisiún)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
South Africa (FPB)	✗*	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓
United Kingdom (Ofcom)	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓

*Information captured is illustrative and non-exhaustive, and reflects regulatory contexts at the time of drafting (April 2024)

Developing common regulatory approaches

By mapping the similarities and differences in our regulatory remits, the Network has identified opportunities in multiple areas to pursue coherence between our respective regimes. These include:

- **Regulatory tools** like risk assessment and transparency reporting. We will share our methodologies and evaluation practices approaches to help ensure our respective regulatory tools represent good practice, and work to develop common metrics to minimise unwarranted divergences between them. For instance, while jurisdictions' risk assessment requirements might differ, there is scope to improve consistency in risk assessment methodology to help streamline compliance.
- **User complaints** functions, and related systems (e.g., researcher access to data mechanisms; trusted flagger programs) that enable us to collect evidence and insight. Those of us collecting user complaints will share our experience and evidence to help identify and compare trends in the nature and prevalence of online harms across regions and in compliance practices and outcomes.

- **Information requests to industry.** We will explore opportunities to coordinate in relation to the types of questions we ask of industry as part of our regulatory activities, including supervision and compliance, to help reduce the compliance burden for platforms and produce more comparable global data that better informs our trend analysis.
- **Safety measures.** We will draw on our experiences of good practice, to identify a common set of reasonable steps services can take to address specific harms and risk factors. For example, we might seek to study how complaints-handling processes can be effective and user-friendly and what kind of user empowerment tools tangibly improve peoples' online experiences.

In the short and medium-term, the Network's priorities are to focus our coordination and coherence efforts specifically on our regulatory approaches and implementation.

We also hope to pursue coordination in other areas over the longer term. For instance, where members are permitted under our respective legal frameworks to receive and act on individual user complaints, coordination and sharing intelligence can ensure they can better assist individuals in cases with an international nexus, such as where the person experiencing harm is in one country, the person targeting them is in another, and the platform in question is domiciled in a third country. Indeed, where there are risks of cross-border harm or where there are instances of systemic non-compliance across jurisdictions, the Network might consider working more closely on investigations and enforcement action.

The Network's activities for pursuing coordination and coherence

The Network has developed its first workstreams aimed at advancing regulatory coordination and coherence amongst members. These include:

- **Our observer programme:** This streamlines and coordinates direct engagement between regulators and the multistakeholder online safety community. The programme enables regulators to draw on the research, expertise, and influence of observers to enhance our work and ensure it is globally relevant, and enables observer organisations from civil society, academia, and government to contribute to our efforts to develop coherent regulatory approaches.
- **Working Groups:** These bring members and observers together to discuss and collaborate on specific issues in online safety regulation, such as age assurance and

generative AI (through the Technology Working Group), and best practices on media and digital literacy and online safety education (through the Education and Awareness Working Group).

- **Regulator dialogues:** Our regular regulator-only meetings provide members with an opportunity to share research, experiences, and lessons learned, including information about online harms trends and our experiences of engaging with regulated services. These exchanges support the development of a common evidence base for our work and better equip members to engage effectively with industry.

Working with others to advance coherence

We recognise that the Network cannot achieve regulatory coherence or mitigate the risks of fragmentation overnight, or indeed by itself. In that context, we intend to work closely with the broader online safety community globally to elevate best practices and lessons across regions and contexts, and support the efforts of other institutions and initiatives that seek to advance global regulatory coherence.

Through the principles and activities outlined in this statement, the Network hopes to support each member in carrying out its statutory functions and exercising its powers, allow members and observers to benefit from peer expertise and best practice, and ensure the development of an international regulatory landscape that provides clarity and coherence, for a safer global digital ecosystem.

Contact current Chair:

ofcom.international@ofcom.org.uk

| www.ofcom.org.uk/about-ofcom/international/online-safety/gosrn

May 2024