

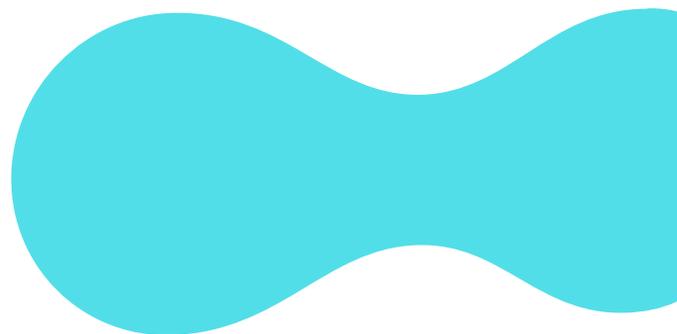
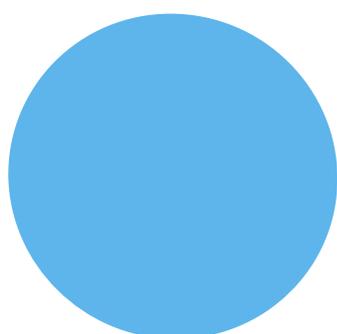
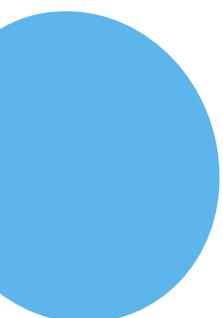


Global
Online Safety Regulators
Network

Terms of Reference 2022 - 2023

The Global Online Safety Regulators Network (the Network) brings together independent regulators to cooperate across jurisdictions. The Network will share information, best practice, experience, expertise and support harmonised or coordinated approaches to online safety issues.

The Terms of Reference outline the rules and procedures that apply to the Network.



Terms of Reference	3
1. Purpose	3
2. Term.....	3
3. Governance.....	3
3.1 Rotating chair.....	3
3.2 Decisions.....	4
4. Structure and composition.....	4
4.1 Members.....	4
4.2 Observer status.....	5
4.3 Joining the Network.....	5
5. Required participation.....	5
5.1 Meetings	5
5.2 Confidentiality of meetings	6
5.3 Member commitments	6
6. Disciplinary actions and termination.....	6
7. Administrative arrangements.....	7
Annex 1 – Charter of Engagement.....	8
Annex 2 – Guidance on interpreting membership and observer criteria.....	9
Online safety.....	9
Human rights, democracy and the rule of law.....	9
Autonomy.....	10

Terms of Reference

1. Purpose

The purpose of the Network is to bring together independent online safety regulators to:

- cooperate across jurisdictions – sharing relevant information, best practice, experience and expertise
- support harmonised or coordinated approaches to online safety issues.

2. Term

This Terms of Reference is effective once agreed by all members. It will be reviewed on an annual basis, with respect to Network growth, and when requested by members. It will remain ongoing until terminated by agreement between members.

3. Governance

3.1 Rotating chair

A Chair and Vice-Chair representing member organisations will be responsible for organising and facilitating the Network's meetings and activities. A representative from Australia's eSafety Commissioner nominates to assume the role of Chair for the first two years. These positions will rotate between members each year, and adhere to the following procedures:

- Chair and Vice-Chairs are appointed for a term of one year, with a maximum of two consecutive years.
- Vice-Chairs will be appointed through voluntary assignment and agreement between members (consensus).
- After serving as a Vice-Chair, the Vice-Chair will become Chair in the following year.

Employees from the organisation in the role of Chair, with support of the Vice-Chair, will fulfil secretariat needs, including:

- convening working-level meetings every two months
- convening quarterly senior executive meetings
- preparing and distributing meeting agendas
- recording and distributing minutes
- facilitating the fair assessment of applications to join the Network.

3.2 Decisions

Decisions can be made on a range of matters, including:

- activities undertaken by the Network, including setting strategic priorities and plans
- reviewing and updating the Terms of Reference or membership criteria
- assessing (accepting or rejecting) requests for membership or observer status (see Term 4.3).

The Network can make a decision where there is consensus among its members. Consensus can be established either through an expression of agreement within correspondence or during meetings. Observers do not have a vote in decisions (see Term 4.2).

Where consensus cannot be reached and a decision is critical for the Network's continued operation, decisions will require two-thirds majority approval. Each jurisdiction may cast one vote only, even if it is represented by more than one member. Members undertake to cooperate and collaborate in order to facilitate discussions, information sharing and knowledge exchange on matters relating to online safety, regulatory remits and outcomes, and standards setting.

4. Structure and composition

The members of the Network are the primary participants. In addition, the Network might have observers. Both are described in the paragraphs below.

4.1 Members

The Network is constituted by members representing the respective online safety regulatory body/bodies in a jurisdiction. The Network will be made up of one senior official and at least one working-level contact from each member.

In addition to the criteria set out below, all members must agree to the Charter of Engagement (see Annex 1).

4.1.1 Membership criteria

Membership of the Network is open to entities that meet the following criteria:

1. A national body with legal powers and duties set out in legislation to perform one or more **online safety** functions, including investigation, enforcement, or education, but excluding purely advisory functions.
2. The entity has **autonomy** protected in law to perform its functions independently of commercial and political interference.
3. The entity is bound by commitments to **human rights, democracy and the rule of law**.¹

¹See Annex 2 for guidance on interpreting the membership criteria.

4.2 Observer status

The Network may give observer status to entities and individuals that do not meet the membership criteria, but that engage in online safety research, advocacy or regulation. Observers may be invited to take part in specific meetings or contribute to certain matters. The status and participation of each observer will be determined by the Network members. Expectations for observers will be included in a separate rules and procedures document.

Observers may include:

- relevant national regulatory bodies supporting the development of online safety legislation
- policy professionals developing online safety legislation
- regional regulatory bodies
- industry representatives and trade bodies or associations
- civil society organisations
- academics, researchers, and individuals or organisations with relevant expertise
- law enforcement
- multilateral groupings with a complementary mandate, such as cyber policy, data protection, privacy, or competition
- other relevant individuals or organisations as agreed by consensus among the members.

4.3 Joining the Network

An entity may apply to be a member of the Network by demonstrating that it satisfies the membership criteria, using an application form submitted to the Chair. Applications for membership, or for observer status, are approved with consensus of all Network members. Evidence or additional information may be requested by the Network members in order to assess the application.

Membership is formalised by agreeing to a Statement of Intent, which affirms the purpose and commitments of the Network, and the Charter of Engagement (see Annex 1). Members will be accountable to the Statement of Intent.

5. Required participation

5.1 Meetings

Engagements will take place through working-level meetings every two months and quarterly senior executive meetings, with members also expected to exchange correspondence between meetings. Meetings will normally occur via videoconference, with the possibility of an annual in-person meeting to be decided by consensus among members.

Failure to attend multiple meetings without excuse or notice might result in a review of membership (see Term 6).

5.2 Confidentiality of meetings

Discussions in meetings will not typically be treated as confidential, unless sensitive information is shared, or where a member or observer expresses a preference for information to be confidential. Where confidential information is shared, such information and any records or documents referring to this information shall not be disclosed to any parties outside of the Network.

The minutes of the Network meetings are confidential. Members may decide to restrict access to some meeting documents to members and exclude observers.

Members and observers shall be required, even after their membership and/or participation has ceased, not to disclose confidential information exchanged during Network meetings or otherwise obtained through engagement with the Network.

5.3 Member commitments

All members commit to:

- attending and actively contributing to Network meetings
- sharing online safety information, trends and updates
- maintaining privacy and confidentiality on information exchanged within the Network
- engaging collaboratively to make sure members' activities are coordinated and aligned
- contributing to an agreed workplan
- rotating as Chair and Vice-Chair, where organisational resources allow, to make sure that secretariat work is distributed.

These commitments will be confirmed by agreeing to the Statement of Intent (see Term 4.3).

6. Disciplinary actions and termination

Members may be subject to disciplinary action should they:

- fail to adhere to their commitments under Section 5 (including participation in meetings, confidentiality, and commitments pursuant to the Statement of Intent)
- fail to adhere to the Charter of Engagement.

Disciplinary action follows a tiered, escalatory process. In the first instance a member may have their voting rights suspended. Termination of membership can then be considered six months after voting rights have been suspended, should the member not have made sufficient attempts to address the issues for which its voting rights were suspended.

A vote on the suspension of voting rights or termination of membership may be called by the Chair if at least two-thirds of members request a vote on the matter. Both votes require consensus of all members (excluding the member that is the subject of the vote).

7. Administrative arrangements

When possible, draft agendas and other meeting documentation will be circulated about two weeks before meetings. Minutes will be provided to members and applicable observers promptly after each meeting.

This Terms of Reference may be amended, varied or modified in writing after consultation and agreement by consensus among members.

A meeting quorum is satisfied where at least half of all members are present.

Contact current Chair:

international@esafety.gov.au

| www.esafety.gov.au/international

| November 2022

Annex 1 – Charter of Engagement

A member's engagement in the Network is underpinned by a commitment to the following values and actions:

- 1.** Advocating for the importance of online safety regulation, working in the public interest and informed by evidence to create a safer and more positive digital environment.
- 2.** Recognising that online harms affect all people regardless of national boundaries.
- 3.** Championing a human rights-based approach to online safety regulation and harm prevention efforts and acknowledging that this will require consideration of a range of fundamental human rights.
- 4.** Pursuing best practice in online safety regulation.
- 5.** Cooperating with other rights-based online safety initiatives, frameworks and principles.
- 6.** Operating in a spirit of openness, to facilitate collaboration and information exchange.
- 7.** Acting independently of commercial and political interference.
- 8.** Seeking diversity in membership to reflect a truly global Network.
- 9.** Appreciating the differences in local contexts and maintaining mutual respect for each other's unique cultures and values.
- 10.** Highlighting the importance of international cooperation to the pursuit of a safer and more positive digital environment and global improvements in online safety.
- 11.** Actively engaging with the Network at both the working and senior levels.

These commitments will be confirmed by agreement to the Statement of Intent (see Term 4.3).

Annex 2 – Guidance on interpreting membership and observer criteria

The membership and observer criteria listed at Term 4 refer to some concepts that are not universally defined, and which might differ between jurisdictions. The guidance below provides further information on how to interpret certain terminology used in the criteria, while giving members more information on assessing applications to join the Network.

Online safety

While the Network’s remit is strictly focused on online safety-related issues, it is acknowledged that each jurisdiction might have a different interpretation of what is considered within the scope of online safety. Therefore, the Network will adopt a broad definition of online safety. This will be based on an understanding of the online safety issues regulated across members’ jurisdictions.

Online safety regulation is to be understood as a distinct but related component of technology regulation, which touches upon issues such as data privacy and cybersecurity, but has a general focus on safety.

Online harms are the consequences of content or behaviour that can damage an individual’s social, emotional, psychological, financial or even physical safety. These harms can also cause damage to society and democracy. These harms can occur as a result of content, conduct, contact or contract risks² and can include a broad range of online activity.

Human rights, democracy and the rule of law

Membership of the Network is conditional upon members being bound by human rights, democracy and the rule of law. Human rights recognise the inherent value of each person, regardless of background, location, appearance, thoughts or beliefs. Human rights are based on principles of dignity, equality and mutual respect, which are shared across cultures, religions and philosophies. Human rights should be protected by the rule of law, which provides a structure through which the exercise of power is subjected to agreed rules, guaranteeing the protection of those human rights.³

The International Institute for Democracy and Electoral Assurances’ ‘Global State of Democracy Indices’ will be used as an indicative measure for a preliminary assessment of a prospective member’s ability to meet human rights, democracy and rule of law criteria.

²<https://core-evidence.eu/posts/4-cs-of-online-risk>

³<https://www.un.org/ruleoflaw/rule-of-law-and-human-rights/>

Prospective members could also demonstrate commitment to human rights and the rule of law online through a written submission, which explains their commitment to respect human rights.

This statement could include support for and adherence to:

- Relevant UN or multilateral Declarations and Agreements.
- General Comment 25 on children’s rights in relation to the digital environment.⁴
- Principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency.

Autonomy

The Network requires members to be free to act independently of political and commercial influence or interference.

Political influence

While there will invariably be differences in the level of government control over members, all members must also have a degree of separation from the government and/or the state in the jurisdiction, such that they can independently exercise their powers. This means that members and their officials are not subject to direction or to arbitrary dismissal from government.

Commercial influence

Members must also be free from commercial influence, particularly in relation to the companies that might be impacted by an entity’s regulatory functions. This excludes mandatory levies that might have been introduced by legislation, as long as the payment does not translate into influence.

Independence from political or commercial actors is demonstrated through the ability to carry out functions and exercise powers without interference. For example, this might include the power to report publicly and the ability to make regulatory decisions independently.

⁴<https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx>