Australian Code of Practice on Disinformation and Misinformation

An industry code of practice developed by the Digital Industry Group Inc. (DIGI).

VERSION 4, IN FORCE 30 MAY 2026

Australian Code of Practice on Disinformation and Misinformation *prepared by Digital industry Group Inc*

Table of Contents

1. Preamble

1.1. *Background:* The *Australian Code of Practice on Disinformation and Misinformation* (The Code) has been developed by the Digital Industry Group Inc. (DIGI), a non-profit industry association that advocates for the interests of the digital industry in Australia. The Code was developed in response to Government policy as set out in *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry,* where Government asked the major digital platforms to develop a voluntary code of conduct outlining what the platforms will do to address concerns regarding disinformation and credibility signalling for news content. The Code also takes into account guidance provided by the *Australian Communications and Media Authority set out in Misinformation and News Quality on Digital Platforms in Australia: A Position Paper to Guide Code Development.* The Code underwent revisions in December 2022, and again in May 2026, taking into account feedback from public consultation.

1.2. *Subject-matter:* Disinformation and misinformation are aspects of a wider, multifaceted social problem which involves a range of offline and online behaviours which propagate information that threatens to undermine established democratic processes or public goods such as public health. Concepts such as "disinformation", "misinformation", and "fake news" mean different things to different people and can become politically charged when they are used by people to attack others who hold different opinions on value-laden political issues on which reasonable people may disagree. The understanding and effects of these concepts varies amongst individuals and is also under-researched.

1.3. *Role of digital platforms:* The digital platforms who have signed this Code recognise their role as important actors within the Australian information ecosystem and have already implemented a range of measures to tackle the propagation of disinformation and misinformation. This Code is designed to express the minimum commitments made by Signatories to address the propagation of Disinformation and Misinformation (as defined in this Code) via digital platforms.

1.4. *Signatories:* This Code may be signed by any digital platform who provides products and services to Australian users and has identified a risk that end-users may propagate disinformation and misinformation online and/or can contribute to reducing the propagation of disinformation or misinformation online in other ways e.g via the development of tools and standards.

1.5. *Minimum Commitments:* All Signatories commit to meet the commitments outlined in section 5.2 including the core objective of providing appropriate safeguards against Harms that may be caused by Disinformation and digital platform

1.6. *Opt-in Commitments* This Code provides Signatories the ability to opt into a range of additional measures and objectives, additional to the minimum commitments outlined in 1.5.

1.7. *Proportionality:* The types of user behaviours, content and Harms that this Code seeks to address will vary greatly in incidence and impact amongst the diverse range of services and products offered by different digital platforms. Accordingly, the commitments made by Signatories to the Code are intended to enable them to take actions which are proportional responses to their commitments under the

Code. Section 6 provides further guidance on the contextual factors that Signatories may take into account in this regard.

1.8. *Scope:* Signatories may take a more expansive approach: Signatories may in their discretion implement policies and processes that contain measures to combat Misinformation and Disinformation on a wider range of content or products and services than is within the scope of this Code.

1.9. *Need for collaboration and cooperation among all relevant stakeholders:* While this Code is intended to apply to digital platforms, the Signatories recognise and emphasise that a range of relevant stakeholders have roles and responsibilities in dealing with Disinformation and Misinformation including public authorities, academia, civil society, influencers, and news organisations. Tackling Disinformation and Misinformation effectively will require concerted effort and collaboration by and among these various stakeholder groups, and not only digital platforms. The Signatories welcome ongoing dialogue with stakeholders about what works well, and what does not.

1.10. *Best Practice Guidance:* The Signatories encourage other participants in the information ecosystem such as other digital services to use this Code as a guide to best practice in developing their own response to the evolving challenges of Disinformation and Misinformation.

1.11. *Flexibility:* The digital industry is highly innovative and diverse, and digital platforms operate vastly different businesses which offer a wide and constantly evolving variety of services and products. As a result, the measures taken by digital platforms to address Disinformation and Misinformation in the context of their respective businesses may vary over time. For example, measures which are taken by a user-generated content platform may differ from those taken by a search engine. To accommodate the need *for* flex*ibility* Signatories *can* choose those measures which are most suitable to address instances of Disinformation and Misinformation in relation to different services and products *subject to this Code.*

2. Guiding Principles

2.1. *Protection of freedom of expression:* Digital platforms provide a vital avenue for the open exchange of opinion, speech, information, research and debate and conversation as well as creative and other expression across the Australian community. Signatories should not be compelled by Governments or other parties to remove content solely on the basis of its alleged falsity if the content would not otherwise be unlawful. Given its subject matter, the Code gives special attention to international human rights as articulated within the Universal Declaration on Human Rights, including but not limited to freedom of speech. Signatories are encouraged to, in developing proportionate responses to Disinformation and Misinformation to be cognisant of the need to protect these rights.

2.2. *Protection of user privacy:* Digital platforms value their users' privacy. Any actions taken by digital platforms to address the propagation of Disinformation and Misinformation should not contravene commitments they have made to respect the privacy of Australian users, including in terms and conditions, published policies and voluntary codes of conduct as well as by applicable laws. This includes respect for users' expectations of privacy when using digital platforms and in private digital communications. Additionally, any access to data for research purposes must protect user privacy.

2.3. *Policies and processes concerning advertising placements:* Digital platforms recognise the importance of having policies and processes in place with respect to advertisement placements on their services and products to reduce revenues that may reach the propagators of Disinformation and Misinformation.

2.4. *Empowering users:* Digital platforms should empower users to make informed choices about digital media content that purports to be a source of authoritative current news or of factual information.

2.5. *Integrity and security of services and products*: Digital platforms should communicate on the effectiveness of efforts to ensure the integrity and security of their services and products by taking steps to prohibit, detect and take action against inauthentic accounts on their services and products whose purpose is to propagate Disinformation.

2.6. *Supporting independent researchers:* Digital platforms recognise the importance of industry support for research efforts by independent experts including academics that can inform on trends and effective means to counter Disinformation and Misinformation. The Code provides various options for digital platforms to participate in independent research initiatives.

2.7. *Without prejudice commitments:* This Code is without prejudice to other initiatives aimed at tackling Disinformation and Misinformation by digital platforms.

3. Glossary

This glossary provides information on some of the key terms used in this Code.

3.1. *Digital Content* is content distributed online on a platform owned and operated by a Signatory to this Code that is targeted at Australian users and includes content that has been artificially produced, manipulated or modified by automated means such as through the use of an artificial intelligence algorithm.

3.2. The aspect of *Disinformation* that this Code focuses on is:

3.2.1.1. Digital Content that is verifiably false or misleading or deceptive;

3.2.1.2. is propagated amongst users of digital platforms via Inauthentic Behaviours; and

3.2.1.3. the dissemination of which is reasonably likely to cause *Harm.*

3.3. *Enterprise Services* is software and services including cloud storage and content delivery services which are designed for the use of a specific organisation.

3.4. *Harm* means harms which pose a credible and serious threat to:

3.4.1.1. democratic political and policymaking processes such as voter fraud, voter interference, voting misinformation; or

3.4.1.2. public goods such as the protection of citizens' health, protection of marginalised or vulnerable groups, public safety and security or the environment.

Note: Harm which poses a credible and serious threat excludes harm that cannot be reasonably foreseen.

3.5. *Inauthentic Behaviour* includes spam and other forms of deceptive, manipulative or bulk, aggressive behaviours (which may be perpetrated via automated systems)

and includes behaviours which are intended to artificially influence users' online conversations and/or to encourage users of digital platforms to propagate *Digital Content*.

Note:inauthentic behaviour can be used to artificially amplify the reach or perceived support for misinformation.

3.6. *Misinformation* means:

3.6.1.1. Digital Content (often legal) that is verifiably false or misleading or deceptive;

3.6.1.2. is propagated by users of digital platforms; and

3.6.1.3. the dissemination of which is reasonably likely (but may not be clearly intended to) cause Harm.

3.7. A *news source* is a journalistic producer of news that has editorial independence from the subjects of its news coverage and is:

3.7.1.1. subject to the rules of the Australian Press Council Standards of Practice or the Independent Media Council Code of Conduct; or

3.7.1.2. subject to the rules of the Commercial Television Industry Code of Practice, the Commercial Radio Code of Practice or the Subscription Broadcast Television Codes of Practice; or

3.7.1.3. subject to the rules of a code of practice other regulatory instrument that specifies standard of editorial practice in another country; or

3.7.1.4. is subject to internal editorial standards that relate to the provision of quality journalism; or

3.7.1.5. provides a publicly accessible mechanism for making requests for corrections or complaints about the quality of its news coverage.

3.8. *Digital advertising services* means paid for digital advertising services where the placement of the advertisement is sold directly by Signatories to advertisers

3.9. *Political Advertising* means paid for advertisements:

3.9.1.1. made by, on behalf of a political party; or

3.9.1.2. that advocate for the outcome of an election, referendum or other Federal, State or Territory wide political process (such as a postal vote) supervised by an electoral management body of the Commonwealth or State and Territory.

3.9.1.3. are regulated as political advertising under Australian law.

3.10. *Professional news* is online material produced by a news source that reports, investigates, or provides critical analysis of:

3.10.1.1. issues or events that are relevant in engaging end-users in public debate and in informing democratic decision-making; or

3.10.1.2. current issues or events of public significance to end-users at a local, regional or national level.

3.11. *Recommender system* means a fully or partially automated system used by an online platform to suggest or prioritise in its online interface specific items of Digital Content to recipients of the service, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of the items of *Digital Content* displayed.

3.12. *Relevant signatories are those that have opted into an outcome. Application of the code should be proportionate to the service as provided under section 6.*

3.13. *Search Engines* consist of software systems designed to collect and rank information on the World Wide Web in response to user queries. Search Engines automate their systems in two ways. First, they use software known as "web crawler," "bots' ' or "spiders' ' to discover publicly available webpages and automatically index and collect information from and about these webpages and internet sites. Second, they use ranking systems to return results in a set of links to websites. These ranking systems are made up of a series of algorithms that are ranked based on many factors such as relevance and usability of pages, expertise of sources, and more. The weight applied to each factor may depend on the nature of the query. "Search Engine" excludes downstream entities that offer search functions on their own platforms, for which the results are powered by third-party search engines, as these downstream entities have no legal or operational control of the search results, the index from which they are generated nor the ranking order in which they are provided.

3.14. *Sponsored content* is a paid arrangement between a social media service and an account-holder under which the social media service promotes content posted on the service beyond the account holder's list of followers in exchange for payment but excludes paid for advertising, for example, paid advertising on search engine**s**.

4. Scope, application and commencement of this Code

4.1. *Scope:* Recognising that the the incidence and impact of the risks posed by Disinformation or Misinformation will vary greatly, amongst the diverse range of services and products provided by Digital platforms in Australia, it is expected that the commitments under this Code will apply primarily to services and products that disseminate Digital Content to end users in Australia where Signatories consider the risk of disseminating Disinformation and Misinformation is material and/or where Signatories consider they can make a material contribution to reducing the impact of Harms arising from Disinformation and Misinformation in other ways e.g. the development of tools and standards. The Code may, therefore, be signed by a broad range of Signatories and a range of products and services, and is not limited to specific types of Digital Content. For example, products services and initiatives in scope of the Code may include those that:

4.1.1.1. disseminate user-generated Digital Content (including shared content); and/or

4.1.1.2. disseminate Digital Content that is returned and ranked by Search Engines in response to user queries;

4.1.1.3. provide technological standards or solutions that aim to assist digital platforms and /or end-users to identify and combat Disinformation and Misinformation;

4.1.1.4. offer sponsored content and/or digital advertising services; and

4.1.1.5. aggregate and disseminate news and other types of journalistic content from a variety of different sources.

Note 1: political advertising is excluded from the scope of Misinformation but may fall within the definition of Disinformation if propagated by Inauthentic Behaviours

Note 2: professional news content disseminated by a news aggregation service is excluded from the definition of Misinformation but may fall within the definition of Disinformation if propagated by Inauthentic Behaviours.

4.2. *Excluded services and products*: The following are not services and products subject to this Code:

4.2.1.1. private messaging services including those provided via software applications;

4.2.1.2. email services including those provided via software applications; C. Enterprise Services.

4.3. The list of services and products that are within the scope of the Code or which are excluded is not intended to be exhaustive as new services and products are likely to emerge, some of which will be relevant to the Code. *Relevant signatories* will identify the relevant products and services covered by this Code in accordance with section 7.

4.4. *Content that is not Misinformation:* The following content is not Misinformation under this Code:

4.4.1.1. content produced in good faith for entertainment (including satire and parody) or for educational purposes;

4.4.1.2. content that is authorised by an Australian State or Federal Government;

4.4.1.3. subject to sections 5.23 to 5.25, Political Advertising or content authorised by a political party registered under Australian law; and

4.4.1.4. professional news content.

Content that falls within this section 4.4 may fall within the definition of Disinformation if propagated by Inauthentic behaviours.

4.5. Signatories may, in their discretion, implement policies and procedures which govern the dissemination by users on their platforms of the types of content excluded from the provisions of the Code concerning Misinformation under section 4.4, where Signatories determine such content is reasonably likely to cause Harm.

4.6. *Application of existing laws*: There are a range of existing laws or regulatory arrangements (such as the *Online Safety Act 2021* (*Cth*)) as well as prohibitions or restrictions concerning matters as diverse as tobacco, therapeutic goods, online gambling, election advertising, and defamation that may overlap with some of the matters covered by the Code. To the extent of any conflict with this Code, those laws and regulations will have primacy.

4.7. *Application*: The commitments made by each Signatory apply to it, in respect of the commitments it adopts, in respect of the products and services it nominates, from the date that it opts into those commitments.

4.8. *Commencement*: This Code commenced on 22 February 2021. Revisions to the Code were made on October 11, 2021 (to reflect new governance arrangements, December 20 , 2022 and *May 30* 2026.

Note: these revisions reflect the outcome of the Code's first and second review.

5. Objectives and Measures

5.1. *General:* This section incorporates a range of measures aimed at achieving the Code's objectives and outcomes which are informed by the purpose and guiding principles set out in section 2 above.

5.2. *Signatories Commitments.* All Signatories commit to the core Objective 1, Outcome 1a of this Code so as to contribute to reducing the risk of Harms that may arise from the propagation of Disinformation and Misinformation on digital platforms and will provide transparency reports as set out in section 7. Not all objectives and outcomes will be applicable to all Signatories who may adopt one or more of the measures set out in this section 5 in a manner that is relevant and proportionate to their different services and products, in accordance with the guidance in section 6. Signatories recognise that measures implemented under the Code may also evolve to reflect changes in their services and products, technological developments and the information environment.

5.3. *Opt-in*: Section 7.1 below outlines how Signatories will elect to opt into the commitments.

5.4. *Terminology of measures*: In implementing measures under the Code, Signatories recognise that actions taken aimed at achieving any outcome including the implementation of policies and processes may use terminology other than "Disinformation" and "Misinformation" and may, for example, refer to or a range of prohibited user behaviours or conduct such as making false or misleading representations about the user's identity, origin or intentions and/or a range of prohibited content such as misleading, deceptive, dangerous or harmful content.

5.5. *Plain language*: Where Signatories commit to publishing their policies, procedures and any relevant community guidelines or additional information on their actions to combat Disinformation and Misinformation, they will use reasonable commercial efforts to do so in plain language and in an accessible, user-friendly format.

5.6. *Restrictions on lawful content or users' access:* In seeking to comply with the requirements of this Code, Signatories are not required to (although they may elect to) take measures that require them to delete or prevent access to otherwise lawful content solely on the basis that it is or may be misleading or deceptive or false. Nor will Signatories be required to signal the veracity of content uploaded and shared by their users.

5.7. *Need for transparency to be balanced against disclosure risks:* Signatories recognise that in implementing commitments to promote the public transparency of measures taken under this Code there is a need to balance the need to be open about those measures with the risk that the release of certain information may result in an increase in behaviours that propagate Disinformation and Misinformation, or which increase its virality.

Objective 1: Provide safeguards against Harms that may arise from Disinformation and Misinformation.

Outcome 1a: Signatories contribute to reducing the risk of Harms that may arise from the propagation of Disinformation and Misinformation on digital platforms by adopting a range of scalable measures.

5.8. *All* Signatories will develop and implement measures which aim to reduce the propagation of and potential exposure of users of digital platforms to Disinformation and Misinformation.

5.8.1. Measures implemented under 5.8, may include, by way of example rather than limitation:

5.8.1.1. policies and processes that require human review of user behaviours or content that is available on digital platforms (including review processes that are conducted in partnership with fact-checking organisations);

5.8.1.2. labelling false content, AI-generated content or providing trust indicators of content to users;

5.8.1.3. demoting the ranking of content that may expose users to Disinformation and Misinformation;

5.8.1.4. removal of content which is propagated by Inauthentic Behaviours;

5.8.1.5. providing transparency about actions taken to address Disinformation and Misinformation to the public and/or users as appropriate;

5.8.1.6. suspension or disabling of accounts of users which engage in Inauthentic Behaviours;

5.8.1.7. the provision or use of technologies to identify and reduce Inauthentic Behaviours that can expose users to Disinformation such as algorithmic review of content and/or user accounts;

5.8.1.8. the development and adoption of standards or the provision or use of technologies which assist digital platforms or their users to label or check the authenticity of or identify the provenance or source of digital content;

5.8.1.9. exposing metadata to users about the source of content;

5.8.1.10. enforcing published editorial policies and content standards;

5.8.1.11. prioritising credible and trusted news sources that are subject to a published editorial code (noting that some Signatories may choose to remove or reduce the ranking of news content which violates their policies in accordance with section 4.5);

5.8.1.12. partnering and/or providing funding for fact checkers to review Digital Content; and

5.8.1.13. providing users with tools that enable them to exclude their access to certain types of Digital Content

5.8.1.14. working with electoral authorities to combat the dissemination of Misinformation and Disinformation about electoral processes, and to address breaches of relevant Commonwealth electoral legislation.

Outcome 1b: Users will be informed about the types of behaviours and types of content that will be prohibited and/or managed by Signatories under this Code.

5.9. *Relevant signatories* will implement and publish policies and procedures and appropriate guidelines or information relating to the prohibition and/or management of user behaviours and/or content that may propagate Disinformation and/or Misinformation via their services or products.

Outcome 1c: Users can report content or behaviours to Signatories that violate their policies through publicly available and accessible reporting tools.

5.10. Relevant signatories will implement and publish policies, procedures and appropriate guidelines that will enable users to report the types of behaviours and content that violates their policies under section 5.9.

5.11. In implementing the commitment in section 5.10, Relevant signatories recognise that the terms Disinformation and Misinformation may be unfamiliar to users and thus policies and procedures aimed at achieving this outcome may specify how users may report a range of impermissible content and behaviours on digital platforms.

Outcome 1d: Users will be able to access general information about Signatories' actions in response to reports made under the Code.

5.12. Relevant signatories will implement and publish policies, procedures and/or aggregated reports (including summaries of user reports made under 5.10) regarding the detection and removal of content that violates platform policies, including but not necessarily limited to content on their platforms that qualifies as Misinformation and/or Disinformation.

Outcome 1e: Users will be able to access information about enforcement action taken against their accounts by Relevant signatories in response to violations of policies.

5.13. Relevant signatories will provide users with information where enforcement action has been taken on their account on the basis of violation of policies under 5.9.

Outcome 1f: Users will be able to access information about the design and operation of Relevant signatories' recommender systems and have options relating to content suggested by recommender systems.

5.14. Relevant signatories that provide services (other than *S*earch *E*ngines) whose primary purpose is to disseminate information to the public and which use recommender systems, commit to :

5.14.1.1. make information available to end-users that describe how they are designed and how platform recommender systems influence the visibility and dissemination of Digital Content including safeguards to limit the propagation of Misinformation; and

5.14.1.2. provide end-users with options that relate to Digital Content suggested by recommender systems that are appropriate to the service.

Note: for example, the comments section provided under news stories published by an online newspaper would be ancillary to the main service represented by the publication of news under the editorial responsibility of the publisher and therefore not subject to this commitment.

Outcome 1g: Relevant Signatories will support users to identify digital content that has been generated by the use of their AI systems on their services.

5.15. Relevant signatories that enable the generation and dissemination of AI generated and manipulated content as part of their service will support users to identify digital content on their service that has been generated by the use of their AI systems, for example by enabling the labelling or marking of AI-generated or manipulated content.

Objective 2: Disrupt advertising and monetisation incentives for Disinformation and Misinformation.

Outcome 2: Advertising and/or monetisation incentives for Disinformation and Misinformation are reduced.

5.16. Relevant signatories that offer digital advertising services will use commercially reasonable efforts to deter advertisers from repeatedly placing digital advertisements that propagate Disinformation or Misinformation.

5.17. Relevant signatories will implement policies and processes that aim to disrupt advertising and/or monetisation incentives for Disinformation or Misinformation.

5.18. Policies and processes implemented under 5.154 may for example, include:

5.18.1. promotion and/or inclusion of the use of brand safety and verification tools;

5.18.2. enabling engagement with third party verification companies;

5.18.3. assisting and/or allowing advertisers to assess media buying strategies and online reputational risks;

5.18.4. providing advertisers with necessary access to client-specific accounts to help enable them to monitor the placement of advertisements and make choices regarding where advertisements are placed; and /or

5.18.5. restricting the availability of advertising services and paid placements on accounts and websites that propagate Disinformation or Misinformation.

5.19. Signatories recognise that all parties involved in the buying and selling of online advertising and the provision of advertising-related services need to work together to improve transparency across the online advertising ecosystem and thereby to effectively scrutinise, control and limit the placement of advertising on accounts and websites that propagate Disinformation.

Objective 3: Work to ensure the integrity and security of services and products delivered by digital platforms.

Outcome 3: The risk that Inauthentic User Behaviours undermine the integrity and security of services and products is reduced.

5.20. Relevant signatories commit to take measures to address user behaviours that are designed to undermine the integrity and security of their services and products, for example, manipulative behaviours and techniques employed by malicious actors such as the use of fake accounts or automated bots that are designed to propagate Disinformation. Signatories will also explore opportunities to cooperate with government and relevant regulatory agencies to identify and address instances of Inauthentic Behaviours that propagate Disinformation on their services.

5.21. To allow for the expectations of some users and digital platforms about the protection of privacy, measures developed and implemented by Relevant signatories in accordance with this commitment should not preclude the creation of pseudonymous and anonymous accounts.

Objective 4: Empower consumers to make better informed choices of digital content.

Outcome 4: Users are enabled to make more informed choices about the source of news and factual content accessed via digital platforms and are better equipped to identify Misinformation.

5.22. Relevant signatories will implement measures to enable users to make informed choices about Digital Content and to access alternative sources of information.

5.23. Measures developed and implemented in accordance with the commitment in 5.21 may include, for example:

5.23.1.1. the use of technological means to prioritise or rank Digital Content to enable users to easily find diverse perspectives on matters of public interest;

5.23.1.2. aggregation or promotion of news content subject to an independent editorial code and complaints scheme;

5.23.1.3. the provision or use of technologies which signal the credibility of news sources, or which assist digital platforms or their users to check the authenticity or accuracy of online news content;

5.23.1.4. the development and deployment of tools to identify the, provenance or source of Digital Content;

5.23.1.5. support for global initiatives and standards bodies (for instance, C2PA) focused on the development of provenance tools

5.23.1.6. the promotion of digital literacy interventions, informed by evidence or expert analysis, for example tools to empower users with context on the content visible on services or that lead users to authoritative sources on topics of particular public and societal interest or in crisis situations or give guidance on how to evaluate Digital Content ; and/or

5.23.1.7. the provision of financial support and/or sustainable partnerships with fact-checking organisations.

Outcome 4a: Signatories cooperate with Federal electoral bodies to support the integrity of federal electoral processes.

5.24. Relevant signatories will promote and support the integrity of Australian federal elections, for example by

5.24.1.1. working with Federal electoral bodies such as the Australian Electoral Commission to implement processes to respond to Digital Content that is likely to mislead or deceive an elector in relation to the casting of a vote; and

5.24.1.2. implementing measures to support access to authoritative sources of information about federal election processes, for example, official government channels of electoral information;

Objective 5: Improve public awareness of the source of Political Advertising carried on digital platforms.

Outcome 5: Users are better informed about the source of Political Advertising.

5.25. While Political Advertising is not Misinformation for the purposes of the Code, *Relevant signatories* will develop and implement policies that provide users with greater transparency about the source of Political Advertising carried on digital platforms.

5.26. Measures developed and implemented by *Relevant signatories* in accordance with the commitment in 5.24 may include requirements that advertisers identify and/or verify the source of Political Advertising carried on digital platforms; policies which prohibit advertising that misrepresents, deceives, or conceals material information about the advertiser or the origin of the advertisement; the provision of tools which enable users to understand whether a political ad has been targeted to them; and

policies which require that Political Advertisements which appear in a medium containing news or editorial content are presented in such a way as to be readily recognisable as a paid-for communication.

5.27. *Relevant signatories* may also, as a matter of policy, choose not to target advertisements based on the inferred political affiliations of a user or choose to define and implement commitments concerning a broader scope of political advertising including advertising that advocates for a political outcome on social issues of public concern.

Objective 6: Strengthen public understanding of Disinformation and Misinformation through support of strategic research.

Outcome 6: Signatories support the efforts of independent researchers to improve public understanding of Disinformation and Misinformation.

5.28. Relevant signatories commit to support and encourage good faith independent efforts to research Disinformation and Misinformation both online and offline. Good faith research includes research that is conducted in accordance with the ethics policies of an accredited Australian University, provided such policies require that data collected by the researcher is used solely for research purposes and is stored securely on a university IT system, or any research which is conducted in accordance with the prior written agreement of the digital platform.

5.29. Measures taken by Relevant signatories to implement 5.27 may include, for example, cooperation with relevant initiatives taken by independent fact checking bodies. Other measures may include funding for research and/or sharing datasets, undertaking joint research, or otherwise partnering with academics and civil society organisations.

5.30. Signatories commit not to prohibit or discourage good faith research, as described in 5.27 into Disinformation or Misinformation on their platform.

5.31. Relevant signatories commit to convene an annual event to foster discussions regarding Disinformation and Misinformation within academia and Civil Society.

Note: The annual event may be conducted via any format (online, offline or a combination) and may cover any topic that is relevant to the Code or its subject matter. The event may, for example, be convened to present or discuss a research initiative of Signatories or the Code administrator.

Objective 7: Signatories publicise the measures they take to combat Disinformation and Misinformation.

Outcome 7: The public can access information about the measures Signatories have taken to combat Disinformation and Misinformation.

5.32. All Signatories will make and publish a transparency report in accordance with section 7.

5.33. In addition, Relevant signatories will publish additional information detailing their progress in relation to Objective 1 and any additional commitments they have made under this Code.

5.34. Relevant signatories may fulfill their commitment in section 5.32 by providing additional reports and/or public updates on areas such as content removals, open data initiatives, research reports, media announcements, user data requests and business transparency reports. Examples of such information could include, by way of example rather than limitation, blog posts, white papers, in-product notifications, transparency reports, help centres, or other websites.

6. Guidance on platform-specific measures

6.1. *Proportionality of measures under Code:* The measures taken by Signatories pursuant to this Code will be proportionate and relevant to their specific context including the Harm posed by instances of Disinformation and Misinformation. Signatories may take into consideration a variety of factors in assessing the appropriateness of measures including:

6.1.1.1. the actors which are engaged in propagating Disinformation and Misinformation;

6.1.1.2. the nature of the behaviour of users propagating Disinformation and Misinformation, for example, whether the behaviour is automated and intentional and/or maliciously motivated and the extent to which it is coordinated, persistent and at scale;

6.1.1.3. the type of Product or Service via which the content is distributed and whether it has network effects that result in content being widely and rapidly shared amongst users of the platform;

6.1.1.4. whether the platform may receive a commercial benefit from the propagation of the content (for example, whether the content is sponsored content);

6.1.1.5. the extent to which it is reasonably possible to verify the falsity of relevant Digital Content via an authoritative or credible source;

6.1.1.6. the proximity and severity of the Harm that is reasonably likely to result from the propagation of the content;

6.1.1.7. the nature of the online community using the digital platfor*m;*

6.1.1.8. the size and nature of the digital platform's business and the resources available to it;

6.1.1.9. the need to protect freedom of expression in balance with other human rights; and

6.1.1.10. the need to protect user privacy.

7. Code administration

7.1. *Opt-in:* In recognition of the variation in business models and product offerings of Digital platforms, this Code is designed to allow a range of businesses to make commitments by way of opt-in arrangements. Within three months of signing the

Code, Signatories will nominate the provisions to which they commit using the Opt-in Nominations Form in Appendix 1. A Signatory is not bound to comply with commitments it has not nominated.

7.2. Each Signatory will annually re-assess the extent the provisions of the Code are relevant to their products and services (including whether any new products and services should be subject to the Code) and update and notify DIGI of any updates to the opt-in form. DIGI will publish updates to the Opt-in Nominations Form on the DIGI website.

7.3. *Withdrawal from Code:* A Signatory may withdraw from the Code or a particular non mandatory commitment under the Code by notifying DIGI.

7.4. *Reporting for All Signatories:* Subject to section 7.5 each Signatory will provide an annual report to DIGI setting out its progress towards achieving the outcomes contained in the Code which will be submitted by May 1 each year, covering the period for the previous calendar year (e.g reports for 2026 calendar year January 1 -December 30 2026 must be submitted by May 1 2027). Each Signatory's annual report will be will be based on (but need not comply with) the Best Practice Guidance for Transparency Reports in Appendix 2 and will:

7.4.1.1. list its product, services or other contributions that are subject to the Code including any additional products or services that it has elected will be subject to the Code during the period covered by the report; and

7.4.1.2. set out its progress towards achieving the Outcomes contained in the Code.

7.5. *Reporting for Signatories that are smaller Digital platforms or who make alternative contributions to the Code:* A Signatory that meets either of the following criteria must submit an initial report to DIGI where its contribution to the Code

7.5.1.1. is not through the provision of a product or service that disseminates Digital Content in Australia; or

7.5.1.2. is as a provider of products or services that dissipates digital Content in Australia that have fewer than one million monthly active Australian end-users.

The Signatory's initial report may be in a format of the Signatory's choosing provided that it sets out:

7.5.1.3. the products, services, or other contributions of the Signatory that are subject to the Code.

7.5.1.4. the Signatory's progress toward achieving the Code's outcomes.

In addition, the Signatory must provide an update to DIGI of its initial report if there have been material changes to the information provided in the report during the period covering any previous calendar year. Material changes for example would include:

7.5.2. the introduction of new products, services, or other contributions that the Signatory has elected to subject to the Code commitments;

7.5.3. any significant expansion in the Australian market of existing products, services, or other contributions that the Signatory that are subject to the Code commitments; and

7.5.4. any changes to the range of measures, policies, procedures, and/or guidelines that materially affect the Signatory's commitments under the Code.

The initial report and any subsequent updates will be submitted by May 1 each year and will be published on the DIGI website.

7.6. *Independent review:* Each Signatory's annual or initial report under the Code will be reviewed by an independent expert appointed by DIGI who will report on Signatories' annual transparency reports under the Code, in order to incentivise best practice and compliance. DIGI will publish the results of the independent expert's review on the DIGI website, together with the Signatories' transparency reports.

7.7. *Complaints:* Signatories have established a complaints facility with an independent Complaints Committee for resolving complaints by the public about possible breaches of Signatories' commitments under the Code. The public can access the complaints facility via a complaints portal on DIGI's website. The DIGI *website also* provides information about the operation of the complaints facility and the governance of the Code. The complaints facility does not accept complaints about individual items of content on Signatories' products or services, which should be directed to the relevant Signatory via their reporting mechanisms.

7.8. *Code Administration:* The Signatories appoint DIGI as the administrator of this Code and have established

7.8.1.1. a Signatory Steering Committee to govern the ongoing development of the Code; and

7.8.1.2. an Advisory Committee of independent members who will meet at not less than six monthly intervals to provide advice to Signatories in accordance with the Advisory Committee's Terms of Reference.

In addition the ACMA provides informal oversight of the Codes and reports to the Government on its assessment of Signatories efforts under the Code.

7.9. *Code Review:*The Code will be reviewed at intervals agreed by the Signatory Steering Committee. The reviews will be based on the input of the Signatories, and on relevant government bodies (including the Australian Communications and Media Authority) and other interested stakeholders including academics and representatives from civil society active in this field. Amendments to the Code will be published on the DIGI website.

7.10. *DIGI Annual Report:* DIGI will produce and publish an annual report on its website concerning the administration of the Code which will include information about any decisions made by the independent Complaints Committee.

Appendix 1: Australian Code of Practice on Disinformation and Misinformation: Opt-in Nominations Form

This form is to be completed by Signatories of the Australian Code of Practice on Disinformation and Misinformation (the Code) to nominate the provisions to which they commit, as required by section 7.1 of the Code. Signatories are bound to comply with the commitments they nominate.

Signatory Information

Field	*Response*
Signatory Name	*Person*
Date of Submission	*Date*
Contact Person	*Person*
Contact Email	*@*

Products and Services Subject to the Code (Section 7.4)

Please list the specific products and services provided to Australian users that are subject to the commitments you are opting into under this Code.

Product/Service Name	*Description/URL (if applicable)*

Mandatory Commitments (Core Objective 1)

Objective 1: Provide safeguards against Harms

All Signatories commit to the core Objective 1, as set out in section 5.2 of the Code.

Objective/Outcome	*Commitment*	*Status*
Objective 1	*Provide safeguards against Harms that may arise from Disinformation and Misinformation.*	*Committed (Mandatory)*

Objective/Outcome	*Commitment*	*Status*
Outcome 1a *(Section 5.8)*	*Contribute to reducing the risk of Harms that may arise from the propagation of Disinformation and Misinformation on digital platforms by adopting a range of scalable measures.*	*Committed (Mandatory)*
Section 7.4	*Provide an annual report to DIGI setting out progress towards achieving the outcomes contained in the Code.*	*Committed (Mandatory)*

Opt-in Commitments (Sections 5.2 and 7.1)

Please indicate the additional Objectives, Outcomes, and specific measures your organisation commits to, beyond the mandatory requirements.

Objective 1: Provide safeguards against Harms (Continued)

Outcome/Section	*Description of Commitment*	*Opt-in? (Yes/No)*
Outcome 1b *(Section 5.9)*	*Users will be informed about the types of behaviours and types of content that will be prohibited and/or managed by Signatories under this Code.*	
Outcome 1c *(Section 5.10-5.11)*	*Users can report content or behaviours to Signatories that violate their policies under section 5.9 through publicly available and accessible reporting tools.*	
Outcome 1d *(Section 5.12)*	*Users will be able to access general information about Signatories' actions in response to*	

Outcome/Section	*Description of Commitment*	*Opt-in? (Yes/No)*
	reports made under 5.9.	
***Outcome 1e** (Section 5.13)*	*Users will be able to access specific information about enforcement action taken against their accounts by Relevant signatories in response to violations of policies under section 5.9.*	
***Outcome 1f** (Section 5.14)*	*Users will be able to access general information about the design and operation use of Relevant signatories' recommender systems and have options relating to content suggested by recommender systems.*	
***Outcome 1g** (Section 5.15)*	*Relevant Signatories will support users to identify digital content that has been generated by the use of their AI systems on their services.*	

Objective 2: Disrupt advertising and monetisation incentives

Objective/Outcome/ Section	*Description of Commitment*	*Opt-in? (Yes/No)*
Objective 2	*Disrupt advertising and monetisation incentives for Disinformation and Misinformation.*	
***Outcome 2** (Section 5.16-5.18)*	*Advertising and/or monetisation incentives for Disinformation and Misinformation are reduced.*	

Objective 3: Work to ensure the integrity and security of services and products

Objective/Outcome/ Section	*Description of Commitment*	*Opt-in? (Yes/No)*
Objective 3	*Work to ensure the integrity and security of services and products delivered by digital platforms.*	
Outcome 3 *(Section 5.19-5.20)*	*The risk that Inauthentic User Behaviours undermine the integrity and security of services and products is reduced.*	

Objective 4: Empower consumers to make better informed choices

Objective/Outcome/ Section	*Description of Commitment*	*Opt-in? (Yes/No)*
Objective 4	*Empower consumers to make better informed choices of digital content.*	
Outcome 4 *(Section 5.21-5.22)*	*Users are enabled to make more informed choices about the source of news and factual content accessed via digital platforms and are better equipped to identify misinformation.*	
Outcome 4a *(Section 5.23)*	*Signatories cooperate with Federal electoral bodies to support the integrity of federal electoral processes.*	

Objective 5: Improve public awareness of the source of Political Advertising

Objective/Outcome/ Section	*Description of Commitment*	*Opt-in? (Yes/No)*
Objective 5	*Improve public awareness of the*	

Objective/Outcome/ Section	*Description of Commitment*	*Opt-in? (Yes/No)*
	source of Political Advertising carried on digital platforms.	
***Outcome 5** (Section 5.24-5.26)*	*Users are better informed about the source of Political Advertising.*	

Objective 6: Strengthen public understanding through research

Objective/Outcome/ Section	*Description of Commitment*	*Opt-in? (Yes/No)*
Objective 6	*Strengthen public understanding of Disinformation and Misinformation through support of strategic research.*	
***Outcome 6** (Section 5.27-5.30)*	*Signatories support the efforts of independent researchers to improve public understanding of Disinformation and Misinformation.*	

Objective 7: Signatories publicise the measures they take to combat Disinformation and Misinformation

Objective/Outcome/ Section	*Description of Commitment*	*Opt-in? (Yes/No)*
Objective 7	*Signatories publicise the measures they take to combat Disinformation and Misinformation.*	
***Outcome 7** (Section 5.31.-5.33)*	*The public can access additional information about the measures Signatories have taken to combat Disinformation and Misinformation.*	

Declaration

On behalf of the Signatory, I confirm that the information provided in this form is accurate and that the Signatory commits to the mandatory provisions and all additional provisions marked 'Yes' in the tables above for the products and services listed.

(Signature)

Please return the completed form to DIGI. The contact details for DIGI are available at DIGI's office address. For any questions regarding this form or the Opt-in process, please contact the Code Administrator at
md@digi.org.au.

Appendix 2: Australian Code of Practice on Disinformation and Misinformation: Best Practice Transparency Reporting Guidelines Version 4.0

Prepared for DIGI by Hal Crawford and updated by DIGI following the 2026 Code review

This document provides guidelines for Signatories preparing the transparency reports required by the Australian Code of Practice on Disinformation and Misinformation ("the Code").

The reports themselves fulfill two functions: to inform the public and to provide a framework for the review of activities under the Code.

These guidelines request Signatories provide:

- *Trended data relevant to the Australian market over extended periods*
- *Clear explanations of major changes in policy*
- *Consistency in reported metrics year-on-year*
- *Audience-friendly documents with a minimum of promotional language*
- *Specific information about efforts to combat AI-generated dis/misinformation*
- *A summary of key data points and qualitative information in the form of a table appended to their report.*

The template follows the same form as the 2022 and 2023 reports, with some additions to reflect the increased scope of the Code from December 2022 and the revisions to the Code made in May 2026.

Introduction

The purpose of this document is to set out guidelines for the annual reporting required of Signatories under the Australian Code of Practice on Disinformation and Misinformation ("the Code"). The annual reports are required under Objective 7 of the Code: "Signatories publicise the measures they take to combat Disinformation and Misinformation."

Signatories filed initial annual transparency reports in May 2021, followed in successive years by reports which have incrementally improved in terms of specificity and consistency.

The general purpose of the reports can be inferred from Objective 7 and the Code's administrative requirements, and is twofold:

- *To communicate to the general public measures taken by Signatories against dis/misinformation*
- *To provide a framework for the independent reviewer, DIGI and other stakeholders to audit compliance with the Code*

Although these aims are related, they could result in significantly different outputs if one function dominated. A key reminder for Signatories is that the documents must be accessible and comprehensible to the general public. The dual purpose of the reports will influence the reporting template recommended in this document.

This is the fourth iteration of these Guidelines following the introduction of Code. This document responds to the expansion of the Code in December 2022, and the revisions to the Code made in May 2026.

Feedback and changes from past reports

Global regulation of dis/misinformation has developed significantly since work on the Australian Code began, and there have been regulatory developments within Australia that may also affect the operation of the Code in future. We focus here on specific requests made to Signatories to improve the utility of their annual transparency reports.

Previous versions of these guidelines asked that signatories:

- *Reduce emphasis on process and policy*
- *Increase use of trended Australia data*
- *Adopt a common reporting period*
- *Use common definitions*
- *Be explicit with objective/outcome commitments*
- *Explain reporting metrics*
- *Provide multi-year metrics reporting*
- *Increase public accessibility*
    - *Observe a word limit (<10,000 words)*
    - *Use breakout case studies*
    - *Use tables, graphs and other visual elements*
- *Reduce promotional tone*

In the 2023 reports two significant additions to the reporting requirements arose from additions to the Outcomes: the introduction of a requirement to provide information about recommender systems (Outcome 1f, previously 1e) and an addition to Objective 2, strengthening the reduction of monetisation incentives for dis/misinformation.

Outcome 1f (previously 1e) gave rise to a reporting obligation to show how signatories have "made information available to the end-user" regarding the operation of recommender engines. Signatories who have committed to this outcome must also include evidence they have made recommender options available to users.

In terms of Objective 2, signatories should speak to their efforts to deter advertisers "from repeatedly placing digital advertisements that propagate Disinformation or Misinformation".

New Outcomes introduced in the May 2026 update which require reporting from 2027 are:

- ***Outcome 1e: Users will be able to access information about enforcement action taken against their accounts by Relevant Signatories in response to violations of policies under 5.10.*** *This requires signatories to provide users with information on enforcement action taken against their accounts for violating policies under 5.10.*
- ***Outcome 1g: Relevant Signatories will support users to identify digital content that has been generated by the use of their AI systems on their Relevant signatories' service.*** *This requires Signatories to implement systems or processes that help users to identify digital content that has been generated by the use of their AI systems on their Relevant signatories' services.*
- ***Outcome 4a: Signatories cooperate with Federal electoral bodies to support the integrity of federal electoral processes.*** *This requires relevant signatories to work cooperatively with*

Federal electoral bodies (e.g., AEC) to promote electoral integrity and increase the accessibility of authoritative information about federal election processes.

Areas for continued improvement are:

- *In the consistent provision of trended data so that comparisons can be made year-on-year*
- *In the provision of data related to the Australian market; and*
- *In clear explanations of relevant internal policy changes.*

In addition, we would like to see discussion and explanation of any measures explicitly undertaken to combat AI-generated dis/misinformation.

Key guidelines

Calendar year reporting

Reports should refer to data from the previous calendar year. The reports filed in May 2027, for example, should relate to the 12 months from 1 January to 31 December 2026. Given that months will have elapsed from the end of that period to the time of compiling the report, it may be acceptable to refer to developments in dis/misinformation in the first half of the current calendar year in passing commentary.

The use of a common reporting period is essential in terms of making comparisons year-on-year and platform-to-platform, and increases the utility of the reports.

Statement of commitments and relevant services/products/platforms

Signatories must state near the beginning of their reports which Code Objectives/Outcomes they have committed to, and which services and products the commitment applies to. This is particularly important for Signatories with big and differentiated portfolios. The omission of a relevant service/product should be noted.

Changes in policy

Signatories should provide details on any significant policy changes related to dis/misinformation and their activities to combat it. This information can be included in the Summary, and in the relevant Outcome sections of the reports. Signatories should clearly explain the change from the old policy to the new, and what prompted the change.

The impact of generative AI

The ACMA has requested Signatories provide information in their transparency reports on specific measures taken to combat dis/misinformation generated by artificial intelligence (AI), which is reflected in the new Outcome 1g. This requirement has led to a structural change to the report template – although the existing Outcomes are engineered to capture activity against this kind of dis/misinformation – but Signatories are directed to consider AI explicitly and provide relevant information under Outcome 1g where available. This also applies to any policy changes that have been instigated by the integration of generative AI on services.

Trended data

In general, there is a need for more trended numerical data in the transparency reports. A minimum of three years of reporting should be supplied with any data, in order to give context. This is a key requirement for understanding.It may not always be possible to supply three years of data for a given metric. In that case, contextualisation through trended monthly numbers may be appropriate.

Accompanying commentary is vital to explain changes. For example, the incidence of detected dis/misinformation may have increased in a given year because the quantum of dis/misinformation increased, or because a Signatory improved detection. Regardless of the potential misinterpretation of trended data, a transparency reporting regime demands it, and furthermore demands that the same data be reported in subsequent years. Any addition or omission of data should also be the subject of an explanatory note.

The expectation of the report review process is that data used as internal Key Performance Indicators in the area of dis/misinformation be included in the report unless there is a clear commercial imperative to omit (see more on KPIs below).

Australian data

Reporting under the Code should provide data for the Australian market. Global metrics may also be relevant, but given the Code's national nature the primary concern should be Australian numbers, examples, and context. It is recognised that Australian data may not always be available: if this is the case, the Signatory should explicitly note that this is the case.

Public accessibility

There are other aspects of the reports that can be built on to improve communication with a general audience:

- *The emphasis on brevity in the first version of these guidelines was perhaps too severe given the big scope of some Signatories' operations. Limiting to 10,000 words should be possible, however.*
- *The use of graphical elements such as bar and line charts helps in communicating numerical information*
- *Breakout (separated from main text body) case studies are recommended to illustrate key points and developments*

Promotional language

One noticeable aspect of some of the first reports was a "promotional" tone. It is natural that Signatories seek to portray their efforts and accomplishments in the best possible light. Unfortunately, promotional language undermines the informational content of the reporting, and encourages cynicism towards what are in fact major and important efforts to curb mis/disinformation. We encourage Signatories to avoid promotional writing and to maintain a neutral stance, highlighting problems and successes with equanimity, and thereby increasing the credibility of the reporting.

We appreciate this can be difficult with a public document: a good rule of thumb is to avoid statements and words that would not be found in internal company reporting.

Generic information

Generic information relating to dis/misinformation process and policy that is unchanged from past reports should be condensed or moved to appendices where appropriate. This is to place greater emphasis on novel aspects of the fight against mis/disinformation, and to avoid losing the novel information among material that is the same year-to-year. The first iteration of these guidelines found that on average, 84% of the content in the initial 2021 reports was generic information relating to dis/misinformation process and policy.

Bearing in mind the dual purpose of the reports – to communicate to the public and demonstrate compliance with the Code – it is necessary to include some of this information repeatedly. For example, it is a mandatory requirement of reporting that Signatories provide links to reporting

mechanisms for dis/misinformation (see below for mandatory links). Signatories may also want to include important information about their approach to tackling dis/misinformation in every report, and there should be an opportunity to do this.

Mandatory links reporting

Signatories' commitments under the Code include simple links to information in order that the independent reviewer may assess compliance. To be explicit regarding these mandatory requirements, they are:

- *1b: Links to user guidelines, policies and procedures relating to mis/disinformation*
- *1c: Links to publicly available tools for reporting mis/disinformation*
- *5: Links to/evidence of published information that allows users to better distinguish factual information from mis/disinformation.*

The link requirements are provided as a checklist to ensure simple elements are not omitted. As indicated in the rest of these guidelines, Signatories are expected to elaborate significantly through the identification and provision of relevant data and commentary. Signatories who have not committed to an Outcome/Objective are exempted from the relevant mandatory elements. Note that in addition to providing these links to assist the independent reviewer, it may be helpful for the reviewer to directly query the Signatory on elements of a submitted report.

The issue of KPIs

In the European Union's 2022 Strengthened Code of Practice on Disinformation, great emphasis is put on quantifying the effectiveness of dis/misinformation countermeasures through Service Level Indicators (SLIs) and Qualitative Reporting Elements (QREs) associated with commitments. The idea is that these data may provide a measure of cross-platform comparison. The EU requires that Signatories provide data for the 6-month reporting period on a country-by-country basis.

In practice, the reports filed under the EU Code demonstrate the difficulty in attempting to mandate meaningful shared metrics between platforms that have very different business models, audiences, interfaces and functions. In the three waves of reports filed to March 2024 , the big platforms have created half-yearly reports over 200 pages long with many incomplete tables, often featuring imprecise or missing data. While it appears that great efforts have been made to satisfy requirements, the documents are of questionable use to the public. They do not include trended data – which will accumulate over time as the corpus grows - and need further aggregation and interpretation before they become useful to anyone.We urge the Australian Code's Signatories to identify and commit to appropriate internal KPIs that are consistently reported on from one year to the next.

Challenges in reporting

The Signatories are diverse businesses and there are big variations in the application of the Objectives/Outcomes. It is not possible to be prescriptive in dictating the data supplied in the transparency reports, although it is expected that Signatories themselves identify relevant data and supply it in line with the suggestions of this document (i.e., within the Australian market, for the reporting period, and for a minimum of two years prior to that). A particular challenge may arise for the Signatories whose dis/misinformation operations are extensive. We encourage them to focus on changes within the reporting period and their interpretations, responses and initiatives. There are also some Signatories whose activities relevant to the Code cannot be quantified. In this case, Signatories are encouraged to report case studies and such qualitative information as will increase the general understanding of their efforts.

Note on formatting

We recommend Signatories use their own formatting conventions in terms of font, layout and colour in the final PDF document. This will not hinder independent review and may enhance messaging to the general public. As implied in the template below, the reports should follow a common structure, with considerable leeway for different elements like graphs, tables and breakout case studies. This will ensure a degree of uniformity across Signatories and better enable comparison between reporting periods. Where numerical data can be supplied, the preference is to present this at the beginning of sections and to contextualise with commentary. It is important to clearly explain metrics and the rationale behind the

Annual Transparency Report Structure

We recommended following the framework below in preparing reports. Content suggestions and constraints are given in brackets. Note the positions of graphs and breakout case studies are given as examples only

Summary

[Discuss in brief the overall features of the reporting period]

[Include analysis of the general environment relevant to dis/misinformation]

[Reiterate the primary elements of your work against dis/misinformation]

[Include information here about significant policy changes related to dis/misinformation]

Commitments under the Code

[Use a table to summarise commitments and the platforms they apply to, as below]

1a [paraphrase Outcome 1a]	*[platform] [service] [product]*
1b [paraphrase Outcome 1b]	*[platform] [service] [product]*
1c [paraphrase Objective 2]	*[platform] [service] [product]*
Etc. …	*Etc. …*

[Include short commentary on omitted objectives/outcomes/platforms/services/products]

Reporting against commitments

Outcome 1a: Reducing harm by adopting scalable measures

[Datpoints/Metrics reported and for what reason]

[Comments on trends observed]

[Any changes in type of content/behaviour targeted]

[Changes to acceptable use policy etc.]

[What measures were successful and how is that reflected in the data?]

[Tables and graphics as appropriate]

[Case studies as appropriate]

CASE STUDY 1 *[Illustrates a particular aspect of data trend or impact of changes made] [Note this is an example location for a case study. If appropriate and available, Signatories should provide several case studies. Such qualitative content is valuable in bringing policy to life.]*

Outcome 1b: Inform users about what content is targeted

[What new initiatives in communicating to users what constitutes mis/disinformation?]

[Evidence of user engagement with this content]

[Links to user guidelines, policies and procedures relating to mis/disinformation]

[Note to include information about work against AI generated mis/disinformation]

[Include any policy changes from the last reporting period]

Outcome 1c: Users can easily report offending content

[Any changes in the way users report content for the reporting period]

[Links to publicly available tools for reporting mis/disinformation]

Outcome 1d: Information about reported content available

[What data have you published to users about the amount and quality of dis/misinformation reporting under 1c?]

[Include such data if available]

[Also give links to where the data has been published]

Outcome 1e: information on enforcement action

[What processes are in place to provide users with specific information on why their accounts were subject to enforcement action for violating policies?]

[What information is provided to the user, and how?]

Outcome 1f: Information about recommender engines

[What information have you provided to users about how recommender engines work on your platforms?]

[What options do users have around recommender engines, and how has that been communicated to them?]

[Provide links where possible, or example screenshots if not]

Outcome 1g: support users identify AI

[What systems and processes have been established that enable users to identify if digital content has been generated by the use of AI systems on your service?]

[how are you addressing: labelling/marking of AI-generated content?]

Objective 2: Disrupt advertising and monetisation incentives for disinformation.

[Explain any data points/metrics as above]

[Quantify progress made against the monetisation of disinformation, graphically if possible]

[what measures have been taken against advertisers who repeatedly provide ads containing dis/misinformation?]

[Changes to policies and processes implemented to reduce monetisation for targeted content and behaviour]

[Any relevant changes in market conditions]

Objective 3: Work to ensure the integrity and security of services and products delivered by digital platforms.

[Detail of work in the period against inauthentic behaviours that impact product security]

[Note to include information about work against AI generated mis/disinformation]

[As above, detail trends and initiatives, and plans in this area]

[This section may contain reference to 1a, given potential overlap in these Objectives – it is acceptable to simply refer to that section if all actions against inauthentic user behaviour are covered there]

[Include any policy changes from the last reporting period]

Objective 4: Empower consumers to make better informed choices of digital content.

[Detail the ways in which you have helped users distinguish dis/misinformation from quality information]

[What is the uptake or awareness of such "empowerment tools"?]

[In what content categories are they active?]

Outcome 4a: cooperation with federal electoral bodies to support the integrity of federal electoral processes

[Detail cooperation with Federal electoral bodies (e.g., AEC) to promote electoral integrity.]

[What measures have been implemented to increase accessibility of authoritative information about federal election processes?]

Objective 5: Improve public awareness of the source of political advertising carried on digital platforms.

[Detail the ways in which you have flagged political advertising and improved the awareness of political sources of advertising]

[Any challenges on the horizon, e.g. Upcoming elections]

***CASE STUDY 2** [Illustrates a particular aspect of data trend or impact of changes made]*

Objective 6: Strengthen public understanding of Disinformation and Misinformation through support of strategic research.

[Suggest the use of the table here]

[Name of university/institute/company]	*[Overview of research]*
…	…
…	…

[Notable success/challenges/changes in the above work]

[Include links]

Objective 7: Signatories will publicise the measures they take to combat Disinformation.

[Aside from this report, what other information about your work against dis/misinformation has been communicated to the public?]

[Quantify engagement with this information if possible]

[Overlaps to some extent with 1d, and if there is complete overlap simply refer to that section]

Concluding remarks

[Unanswered questions and challenges]

[Summary of any new initiatives not already mentioned]

[Evolution of your business's understanding of the problem and how to tackle it]

[Observations on the Code and the process of reporting]

[May include developments between the end of the reporting period and now]

Appendix to report

The Appendix to the report should include a summary of quantitative and qualitative data for relevant Signatories At-Risk of Disseminating Misinformation and Disinformation. The following tables present recommended data points for the relevant reporting period.

Part 1: Quantitative Datapoints

This Part 1 data points relating to the Relevant signatories efforts to address misinformation and disinformation. Relevant signatories are asked to provide information that applies to each type of service they offer that is in scope of the Code.

No.	*Information sought for relevant reporting period*
1. Actions on violations	*Does the signatory have data point/s that demonstrate actions taken with respect to content and/or accounts that violate the relevant service/s' policies that prohibit or manage misinformation or disinformation, and is this AU specific or not?*
2. Media literacy	*Does the signatory have data point/s regarding efforts to enable users to critically engage with sources of information on its relevant services e.g labelling, and is this AU specific data or not?*
3. Effectiveness	*Does the signatory have data point/s that demonstrate the effectiveness of relevant service/s' efforts to manage mis and disinformation on its services?*

Part 2: Qualitative data points

Signatories are only expected to include information against the outcomes and measures below that are applicable to their service. This part is intended to supplement qualitative information largely already provided by signatories in their annual transparency reports to provide greater consistency and comparability.

Objective 1: Provide safeguards against harms that may arise from disinformation and misinformation

Code Outcome 1a: Signatories contribute to reducing the risk of harms that may arise from the propagation of disinformation and misinformation on digital platforms by adopting a range of scalable measures .

Policies

No.	*Information sought for relevant reporting period*
4. Disinformation policies	*Does the signatory have policies that prohibit disinformation/inauthentic behaviour on relevant service/s, and if yes, include relevant information including links to relevant documentation, where available?*
5. Misinformation Policies	*Does the signatory have policies that prohibit misinformation, and if yes, include relevant information*

No.	*Information sought for relevant reporting period*
	including links to relevant documentation, where available?
6. Labelling policies	*Does the signatory have specific policies that restrict (e.g by requiring labelling) artificially produced or manipulated content including AI generated material, and if yes, include relevant information including links to relevant documentation, where available?*
7. Policy changes	*Does the signatory have changes in the service's policies in 1-3, and if so, are the principal changes published?*

Compliance and enforcement

No.	*Information sought for relevant reporting period*
8. Systems and processes for policy compliance	*Does the signatory deploy systems and processes to review user behaviours or user generated content for compliance against the relevant service/s' policies on misinformation or disinformation, and include relevant information including whether human or automated systems and processes or a combination are used with links to relevant documentation, where available?*
9. Human resources	*Does the signatory have dedicated human resources to review UGC content for compliance against the relevant service/s' policies on misinformation or disinformation, and if yes, include relevant information including links to relevant documentation, where available?*
10. Enforcement	*Does the signatory have systems and processes that set out how it enforces compliance by end-users with the relevant service/s' policies on misinformation or disinformation, and if yes, include relevant information*

No.	*Information sought for relevant reporting period*
	including links to relevant documentation, where available?
11. Promotion of reliable sources	*Does the signatory take steps to actively recommend/promote reliable sources of content to active Australian end-users of the relevant service/s, and if yes, include relevant information including links to relevant documentation, where available?*
12. removing/demoting/downranking of violative content	*Does the signatory take steps to remove/demote or downrank content that violates the service's policies/terms of service concerning disinformation/misinformation, and if yes, include relevant information including links to relevant documentation, where available?*
13. Human rights	*How does the relevant signatory promote human rights in implementing code commitments?*

Code Outcome 1B: Users will be informed about the types of behaviours and types of content that will be prohibited and/or managed by Signatories under this Code.

No.	*Information sought for relevant reporting period*
14. End-user information	*Does the signatory publish information that is accessible to Australian end-users, about the types of behaviours and types of content that will be prohibited and/or managed by the signatory under the Code?*
15. Notification of action against users' accounts	*Does the signatory notify active Australian end-users of the service when action is taken against their account, or content they publish on the relevant service/s, for violating the service's policies that prohibit or manage disinformation and misinformation, and if yes, include relevant information including links to relevant documentation, where available?*

No.	*Information sought for relevant reporting period*
16. Review of account action	*Does the signatory allow active Australian end-users of the service to seek a review of action taken related to the violation of the service's policies that prohibit or manage disinformation and misinformation, and if yes, include relevant information including links to relevant documentation, where available?*
17. Fact checking	*Does the signatory invest in fact-checking e.g (partnerships with fact-checking organisations) or other types of collaborative partnerships that aim to support its efforts under the ACPDM, and if yes, include relevant information including links to relevant documentation, where available?*

Code Outcome 1C: Users can report content or behaviours to Signatories that violate their policies.

No.	*Information sought for relevant reporting period*
18. Reporting of policy violations	*Does the signatory allow all Australian users of the service to report user-generated content/or on-platform activity for violating the relevant service/s' policies on misinformation/disinformation, and if yes, include relevant information including links to relevant documentation, where available?*
19. Scope of reporting options	*Does the signatory provide reporting options available to active-Australian end-users that cover all content available on the relevant service/s (e.g both UGC and advertising)?*

Code Outcome 1D: Users will be able to access general information about Signatories' actions in response to reports.

No.	*Information sought for relevant reporting period*
20. Information about response of Signatory to reports	*Does the signatory give active Australian end-users access to general information about the signatory's actions in response to reports about the relevant service/s, and if yes, include relevant information including links to relevant documentation, where available?*

Code Outcome 1E: Users will be able to information about Signatories' actions in response to violations of their policies.

No.	*Information sought for relevant reporting period*
21. User information about account actions	*Does the signatory provide users with information where their accounts on relevant service/s have been subject to enforcement action for violating mis/disinformation policies, and if yes, include relevant information including links to relevant documentation, where available?*

Code Outcome 1F: Users will be able to access general information about Signatories' use of recommender systems and have options relating to content suggested by recommender systems.

No.	*Information sought for relevant reporting period*
22. Recommender systems design and operation	*Does the signatory give active Australian end-users access to general information about the signatory's design and operation of recommender systems on relevant service/s, and if yes, include relevant information including links to relevant documentation, where available?*
23. Customisation options on recommender systems	*Does the signatory provide active Australian end-users with in-service options to customise the content suggested by recommender systems (e.g to restrict content suggestions), and if yes, include relevant*

No.	*Information sought for relevant reporting period*
	information including links to relevant documentation, where available?
24. Tools to block/ mute content	*Does the signatory offer active Australian end-users tools to block or mute content posted by other accounts on the service, and if yes, include relevant information including links to relevant documentation, where available?*
25. Options to users to make changes to recommended content	*Does the signatory offer options in relation to content suggested by recommender systems that enable active Australian end-users to make changes based on topics, themes or narratives suggested by recommender systems used by the service, and if yes, include relevant information including links to relevant documentation, where available?*

Code Outcome 1:G Relevant signatories that enable the generation and dissemination of AI generated and manipulated content as part of their service will support users to identify digital content on their service that has been generated by the use of their AI systems

No.	*Information sought for relevant reporting period*
26. AI systems on signatory's services	*Does the signatory develop or operate AI systems that disseminate AI generated and manipulated content through any of its relevant services?*
27. Assistance to users to identify AI manipulated content	*Does the signatory take steps to assist users identify digital content that has been manipulated by AI systems on their relevant service/s e.g requirements for use of AI systems such as labelling or marking, and if yes include relevant information including links to relevant documentation, where available?*

Objective 3: Work to ensure the integrity and security of services and products delivered by digital platforms

Code Outcome 3: The risk that Inauthentic User Behaviours undermine the integrity and security of services and products is reduced.

No.	***Information sought for relevant reporting period***
28. Integrity and security of services	*Does the signatory have measures in place on the service which prohibit the types of user behaviours that are designed to undermine the integrity and security of the relevant service/s (inauthentic user behaviour), and if yes, include relevant information including links to relevant documentation, where available?*
29. Types of inauthentic behaviours signatory acts against ***30.***	*Does the signatory list the inauthentic user behaviours acted against in Australia such as fake accounts, bot-driven amplification, or artificial reach for disinformation, and provide relevant information including links to relevant documents, where available?*
31. Actions for inauthentic behaviour policy violations	*Does the signatory take actions against content or end-users/accounts that violate their policies concerning inauthentic behavior, and include relevant information including links to relevant documentation, where available?*

Part 3: Additional Reporting

Objective 7: Signatories will publicise the measures they take to combat Disinformation.

Outcome 7: The public can access information about the measures Signatories have taken to combat Disinformation and Misinformation

No.	***Information sought for relevant reporting period***
32. Additional reporting of inauthentic behaviours ***33.***	*Does the signatory provide additional reporting steps taken to tackle disinformation e.g reports under the EU code on actions taken against bot-driven amplification, fake accounts, and deep fakes?*

No.	***Information sought for relevant reporting period***
34. Ad hoc reporting	*Does the signatory provide any additional ad hoc reporting in times of crisis e.g during wars such as the war in the Ukraine?*