Code of Practice

Online Safety Code for dating services

July 2024

1 Introduction

1.1 Purpose

(1) The purpose of this Code of Practice (**Code**) is to establish appropriate safeguards to ensure the safety of individual end-users using dating services. Providers of these dating services have a role to play in addressing the risk of online enabled harm that the community may experience through the use of dating services.

(2) This Code sets out the process for industry participants to follow in order to identify and adopt reasonable compliance measures to minimise the risk of online enabled harm to end-users, regardless of whether this harm occurs online or in the physical world. End-users may be subject to content or conduct from other end-users:

(a) which may result in sexual misconduct;

(b) which may cause them to suffer serious mental or physical harm through their online interactions or in the physical world; or

(c) which may be with the intent of the other end-user gaining online or physical world access to children for the purposes of engaging in exploitation or abuse or committing child sexual exploitation and abuse online or in the physical world.

(3) This Code is a voluntary code of practice which is binding on industry participants, and this Code does not set out all of an industry participant's statutory obligations under Australian law. However, all industry participants commit to complying with their obligations which may apply under all relevant Australian laws.

1.2 Development

This Code has been developed in consultation with the following stakeholders:

(1) an industry working group representing dating services operating in Australia;

(2) the Australian Government as represented by the eSafety Commissioner (**eSafety**) and the Department of Infrastructure, Transport, Regional Communications and the Arts; and

(3) relevant non-government stakeholders.

1.3 Scope

This Code applies to providers of dating services which have voluntarily agreed to comply with this Code, so far as those services are provided to end-users in Australia (**industry participants**).

2 Definitions and interpretation

2.1 Definitions

Unless otherwise indicated, terms used in this Code have the meanings set out below:

(1) **appropriate** where used to qualify measures required under this Code means that when implemented by providers of a dating service, the measures must be demonstrably reasonable, taking into account:

(a) the importance of the online safety objectives specified in this Code;

(b) the importance of protecting Australian end-users from online enabled harm;

(c) the function, purpose, size/scale and maturity as well as the capacity and capabilities of the industry participant providing the dating service; and

(d) any other considerations that may be set out in this Code.

(2) **Australian end-user** means an end-user in Australia.

(3) **Australian law** means an Act of an Australian jurisdiction (including any regulations or instruments made under such an Act), or any other law in force in an external Territory.

(4) **BOSE** means the basic online safety expectations prescribed in the *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth) as amended by *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024 (Cth)*.

(5) **code oversight body** means the code oversight body established under section 8.5.

(6) **dating service** means a relevant electronic service the primary functionality of which is:

(a) to solicit, offer, promote or provide access to dating, relationship, compatibility, matrimonial, social or romantic referral services; and

(b) to enable end-users to communicate with other end-users online,

but does not include such a service to the extent that its functionality is to connect end-users who offer their services for payment.

Note: Examples of services for payment are escort or sex worker services

(7) **end-user** means a natural person who is registered with a dating service provided by an industry participant.

(8) **eSafety** means the eSafety Commissioner (https://www.esafety.gov.au/).

(9) **external Territories** means Ashmore and Cartier Islands, Christmas Island, the Cocos (Keeling) Keeling Islands, the Coral Seas Islands, the Australian Antarctic Territory, the Territory of the Heard and McDonald Islands, and Norfolk Island.

(10) **genuine complaint or report** means a complaint or report about an end-user's conduct or content which:

(a) relates to one or more incidents of online enabled harm or may constitute a serious violation of a dating service's online safety policies;

(b) is made in good faith; and

(c) is not frivolous or vexatious.

(11) **industry participant** has the meaning given to that term in section 1.3.

(12) **moderate** or **moderation** means the act of reviewing end-user generated content or conduct to detect, identify or address reports of content or conduct that may violate applicable Australian laws or a dating service's online safety policies or terms and conditions. Moderation systems can rely on human and/or automation technology to review this content or conduct.

(13) **online enabled harm** means any online or physical world activity between end-users which:

(a) occurs between end-users who were first or primarily socially introduced through a dating service;

(b) results in:

(i) sexual misconduct against a participating end-user or other directly impacted individual; or

(ii) serious non-sexual harm to a participating end-user; and

(c) includes any attempt by an end-user to gain online or physical world access to children through another end-user for the purposes of engaging in exploitation or abuse and/or committing child sexual exploitation and abuse online or in the physical world.

Serious harm in the context of section 2.1(13)(b)(ii) must be considered objectively, and must relate to harm which goes beyond emotional reactions such as those of only distress, grief, fear or anger.

Note: The concept of 'serious harm' is derived from eSafety regulatory guidance on the Adult Cyber Abuse Scheme (updated December 2023). The definition of 'online enabled harm' is intended to capture non-physical harm which is also considered to be serious harm.

For the purpose of this Code, serious harm excludes purely financial harm, defamatory material that causes purely reputational harm, or incidental harm experienced by an end-user as part of social or community interaction. For example, making false statements about an end-user's criminal history will not meet the threshold.

(14) **online safety feature** means any function or functionality offered by a dating service to their end-users which minimises the risk of online enabled harm occurring to these end-users.

(15) **online safety policy** means any systems, processes and policies which are used by a dating service to set the expectations and rules for the dating service and respond to the occurrence of online enabled harm to their end-users. Online safety policies include a dating service's terms and conditions, community guidelines as well as any policy or communication with end-users which incorporate online safety requirements.

(16) **OS Act** means the *Online Safety Act 2021* (Cth).

(17) **Privacy Act** means the *Privacy Act 1988* (Cth).

(18) **related body corporate** has the same meaning given to this term in section 9 of the *Corporations Act 2001* (Cth).

(19) **Safety by Design principles** means the online safety principles developed by eSafety to safeguard users of online platforms and services (https://www.esafety.gov.au/industry/safety-by-design).

(20) **service compliance rating** has the meaning given in section 3.2(1).

(21) **sexual misconduct** means online enabled harm relating to sexual harassment, abusive and threatening language, online stalking, sexual assault or coercion, reproductive or sexual health related abuse, image-based abuse, grooming of end-users to access children for the purposes of engaging in exploitation or abuse or committing child sexual exploitation and abuse, or similar harms all of which are of a sexual nature.

2.2 Interpretation

(1) In this Code, unless the contrary intention appears:

(a) where a term is defined in bold, it has that meaning;

(b) headings are for convenience only and do not affect the interpretation of this Code;

(c) words in the singular include the plural, and vice versa;

(d) where a word or phrase is defined, its other grammatical forms have a corresponding meaning; and

(e) mentioning anything after the word “include”, “includes” or “including” does not limit what else may be required.

(2) In this Code, where examples are provided of the manner in which a requirement of a particular provision of this Code may be satisfied, these examples should not be read as requiring or limiting the manner in which the relevant provision may be satisfied.

3 Compliance

3.1 General requirements

Industry participants must comply with all requirements specified in this Code.

3.2 Compliance rating

(1) Each dating service which is subject to this Code will be rated for its compliance with certain requirements specified in this Code (**compliance rating**). The dating service will need to publish on its service which compliance rating (that is, exceeds, complies with, or partially complies with the standards set out in this Code) it falls within.

(2) A self-assessment of the dating service’s compliance rating will be undertaken by the relevant industry participant, and verified by the code oversight body. In assessing the extent to which a dating service complies with this Code, the dating service shall determine whether they exceed, complies with, or partially complies with the standards set out in this Code. Examples of factors which may be taken into account as to whether a dating service exceeds, complies with, or partially complies with the standards set out in this Code are set out in the table below:

Factors to consider
TIER ONE: A dating service will fall within this category where it exceeds the requirements set out in this Code including in respect of the following: • Section 4.1: Existing systems, processes and policies have been assessed by the industry participant as fully compliant with the Safety by Design principles. Development of future systems, processes and policies will comply with the Safety by Design principles. • Section 4.1: The dating service's online safety features for Australian end-users are the same or similar as for all other end-users (regardless of their location or whether their registration to the service is through a paid subscription), so long as such features are reasonably available and technically feasible in Australia. • Section 5.2: The dating service uses automation technology (which may include AI technology) under human oversight for detection and moderation. • Section 5.3: End-user content which meets certain criteria is automatically blocked or removed. • Section 5.4. If an industry participant operates more than one dating service, any enforcement action taken against an end-user for a serious violation of the online safety policies is applied to all known accounts used by that end-user. • Section 6.3: The dating service publishes information about support resources which are relevant to Australian end-users, and it takes active steps to ensure the complainant is aware of this information. • Section 7.4: The industry participant regularly engages with other industry participants and external stakeholders to assist with the continuous improvement of its systems, processes and policies.
TIER TWO: A dating service will fall within this category where it meets the requirements set out in this Code including in respect of the following: • Section 4.1: Existing systems, processes and policies have been assessed as substantially compliant with the Safety by Design principles. Future systems, processes and policies will substantially comply with the Safety by Design principles. • Section 4.1: The dating service's online safety features for Australian end-users are the same or similar as for all other end-users (regardless of their location or whether their registration to the service is through a paid subscription), so long as such features are reasonably available and technically feasible in Australia. • Section 5.2: The dating service uses automation technology (which may include AI technology) for detection and moderation with minimal human intervention/involvement. • Section 5.3: End-user content which meets certain criteria is automatically blocked or removed. • Section 6.3: The dating service publishes information about support resources which are relevant to Australian end-users, but it does not take any active steps to ensure the complainant is aware of this information. • Section 7.4: The industry participant relies solely on its engagement with other industry participants to assist with the continuous improvement of its systems, processes and policies.
TIER THREE: A dating service will fall within this category where it does not meet at least one of the requirements set out in this Code, which may include the following: • Section 4.1: No assessment has been made as to whether existing systems, processes or policies are compliant with the Safety by Design principles. Future systems, processes and policies may not comply with the Safety by Design principles. • Section 4.1: The dating service's online safety features may be limited for Australian end-users compared to other end-users (whether by regional lockout or providing advanced features for paying subscribers only). • Section 5.2: The dating service only uses non-AI automation technology for detection and moderation with no human intervention/involvement.

- Section 5.3: End-user content is blocked or removed only after a complaint has been made, and the industry participant has investigated the complaint.
- Section 6.3: The dating service publishes information about support resources which may not be entirely relevant to Australian end-users and it does not take any active steps to ensure the complainant is aware of this information.
- Section 7.4: The industry participant does not engage with other industry participants, or have any arrangements with external stakeholders, to assist with the continuous improvement of its systems, processes and policies.

(3) The code oversight body will publish the compliance rating for all dating services which are subject to this Code, and which has been verified by the code oversight body.

3.3 Lawful conduct

Nothing in this Code prohibits an industry participant from engaging in conduct which is ordinarily unlawful, if a lawful exception, exclusion or protection from liability exists under Australian law and applies to that industry participant's conduct.

3.4 No breach of this Code where action is required under another Australian law

An industry participant will not be in breach of this Code if it is bound by another Australian law which requires the industry participant to act, or not act, in a way which is contrary to its obligations under this Code.

Note: For example, an industry participant's obligations under this Code may be subject to its privacy obligations under the Privacy Act 1988 (Cth).

4 Online safety frameworks and other statutory obligations

4.1 Online safety frameworks

(1) This Code has been developed to promote the development and operation by dating services of online safety frameworks that have been developed by the Australian Government to protect the Australian community from online enabled harm.

(2) This Code requires industry participants to meet the following objectives:

(a) understand the online safety risks in respect of their dating service and take active steps to mitigate potential misuse of their service and reduce their users' potential exposure to online enabled harm;

(b) give users a level of empowerment and autonomy to manage their online safety in a way that aligns with their own interests and supports safe online interactions; and

(c) are reasonably transparent and accountable in how their online safety features and online safety policies work and the steps they are taking to continuously improve these features and policies, and how they are educating and empowering users about the steps that users can take to address online safety concerns.

(3) An industry participant must have regard to their obligations under this Code in the development and operation of their dating service, as well as the following online safety frameworks:

(a) expectations prescribed in the BOSE;

(b) Safety by Design principles; and

(c) the Five Country Ministerial Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (https://www.weprotect.org/library/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse/).

4.2 Other statutory obligations

Notwithstanding the requirements which are set out in this Code, industry participants must ensure they comply with any statutory requirements set out in an applicable industry code or industry standard registered by eSafety.

5 Online safety of end-users

5.1 Terms and conditions to refer to prohibited content and conduct

Dating services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided to the recipients of the service, in their terms and conditions. The terms and conditions must as a minimum prohibit the upload of illegal content (which includes sexual misconduct) and non-consensual intimate images.

5.2 Detection, moderation and investigation

(1) An industry participant must implement appropriate systems, processes and policies which allows, to the extent reasonably practicable based on the technological capability of its dating service, for the:

(a) detection of potential incidents of online enabled harm involving Australian end-users; and

(b) enforcement of the dating service's online safety policies, including the moderation of content to comply with the online safety policies of the dating service.

(2) An industry participant must implement appropriate systems, processes and policies to review:

(a) complaints made by an end-user which relate to online enabled harm (refer to section 6); or

(b) any detected incidents which may violate its online safety policies (refer to section 5.2(1)).

5.3 Blocking and removing content

Any industry participant must implement appropriate systems, processes and policies to block or remove content from end-user profiles which may have violated its online safety policies. The extent of any end-user content which is blocked or removed will be subject to the relevant dating service's moderation guidelines and technology capabilities, and may include blocking or removal of an end-user's profile, or specific content such as text and media where such granularity is technologically feasible for a dating service.

5.4 **Actions against non-compliant end-users**

(1) An industry participant must implement appropriate systems, processes and policies which:

(a) provide appropriate guidance to the industry participant's personnel on the steps that should be taken when a complaint is made or when a potential incident of online enabled harm has been detected;

(b) includes clear internal channels for the industry participant's personnel to escalate and prioritise reports of violations of its online safety policies;

(c) allows the industry participant to take appropriate action against an end-user which has been found to have violated its online safety policies; and

(d) allows the industry participant to identify whether an end-user who has been banned from, or whose account has been terminated by, a dating service, is creating new accounts for that dating service and if so, take reasonable steps to delete or otherwise block that end-user from accessing that dating service.

(2) The actions which may be appropriate to take against an end-user under section 5.4(1)(c) for a confirmed or detected/suspected violation of an industry participant's online safety policies include (where applicable):

(a) terminating the end-user's account if they have been found by the industry participant to have committed a serious violation of its online safety policy; and

(b) limiting the functions of, or suspending, the end-user's account for a defined period if they have been found by the industry participant to have committed a less serious violation of its online safety policy.

(3) If the industry participant:

(a) operates more than one dating service (including any dating services operated by a related body corporate); and

(b) has terminated an end-user's account as set out in section 5.4(2)(a) on the grounds the end-user has been determined by the industry participant to have committed a serious violation of its online safety policies,

the industry participant must take the same action against that end-user's accounts and profiles on all other dating services operated by the industry participant or its related bodies corporate to the extent possible.

5.5 **Deleting end-user accounts**

If:

(1) an end-user of a dating service requests the permanent deletion of their account; or

(2) an industry participant has determined that an end-user's account is to be terminated under section 5.4(2)(a) or for any other reason determined by the industry participant,

the industry participant must implement appropriate systems, processes and policies to retain the information contained in that account for an appropriate period of time (having regarding to data retention laws and other matters) after the request or determination is made, before the information in the account is permanently deleted or terminated.

Note: For example, a dating service may determine that it wishes to retain information relating to an end-user's account (including interactions with other end-users such as messages and chat histories) for up to 90 days following an end-user's request for deletion of their account, and retain the end-user's information for a longer period if the end-user has been banned or their violation of the online safety policies is of a very serious nature.

6 Complaints and reports handling

6.1 Complaints and reports mechanism

(1) An industry participant must implement an appropriate complaints and reports mechanism that enables Australian end-users to make complaints and reports about:

(a) conduct by an end-user of the dating service which may relate to online enabled harm;

(b) how the industry participant handles a complaint made under this section 6; and

(c) any other aspect of the industry participant's compliance with this Code.

(2) The complaints and reporting mechanism must:

(a) be prominently displayed on the dating service;

(b) be transparent about how complaints are handled;

(c) be explained in clear and easy to understand language that the end-user can reasonably understand; and

(d) meet the web accessibility standards set out in section 7.3(2).

6.2 Review of complaints and reports

(1) Unless otherwise specified in this Code, an industry participant must:

(a) review and act on every genuine complaint or report of a potentially serious violation of its online safety policies that is made to it, unless the complaint appears to be frivolous or vexatious or otherwise not made in good faith;

(b) take reasonable steps to complete the review expeditiously and make a determination on the appropriate action to take on the complaint or report; and

(c) if the complaint or report relates to matters involving sexual misconduct or serious violations of the dating service's online safety policies, notify the complainant of the outcome, taking into account the subject matter of the complaint, any ongoing risk of online enabled harm to the complainant, and any legal restrictions that may prevent the disclosure of certain information to the complainant.

(2) An industry participant must retain all information used by it for a review conducted under section 6.2(1) for at least 12 months after the review has been completed and/or the matter has been referred to another party (refer to sections 6.4 and 6.5).

6.3 **Support resources for complainants**

(1) An industry participant must provide complainants with appropriate support resources if they have made a complaint or report against another end-user which relates to matters of sexual misconduct or serious violations of any online safety policies.

(2) The support resources provided to complainants should, as a minimum:

(a) be relevant to the nature of the complaint;

(b) be provided in clear and easy to understand language that the end-user can reasonably understand and which meets the web accessibility standards set out in section 7.3(2); and

(c) have been developed in consultation with appropriate online safety experts or advocacy organisations.

(3) The support resources which are provided to Australian end-users should include those support resources identified by the code oversight body under paragraph 2.1(1)(d) of Appendix A.

6.4 **Referral of complaints to other industry participants**

Industry participants acknowledge that eSafety would like industry participants to consider ways of identifying users who might pose an increased risk of committing a serious violation of the online safety policies of other industry participants. All industry participants agree to work with other industry participants and the Australian Government to investigate options, including through the provision of government-held information to industry participants, to enable industry participants to share information about these end-users.

6.5 **Referral of complaints to law enforcement agencies**

(1) An industry participant must:

(a) establish a clearly identifiable electronic point of contact for Australian law enforcement agencies to request information which is reasonably necessary for the conduct of one or more enforcement-related activities involving online enabled harm. The industry participant's point of contact must be reasonably available to law enforcement agencies to be able to assist, or provide information to, law enforcement authorities; and

Note: For example, an electronic point of contact may include an online safety email address, or a web portal which law enforcement agencies can use to request information from an industry participant.

(b) take reasonable steps to act on information received from Australian law enforcement agencies about an end-user, to the extent possible in accordance with the industry participant's online safety policies and if such steps are not prohibited by any applicable Australian law.

(2) For the purposes of section 6.5(1)(a), an industry participant will disclose information about an end-user to an Australian law enforcement agency if:

(a) the disclosure is required or authorised by an Australian law;

(b) the disclosure is required or authorised by an Australian court or tribunal; or

(c) sections 6.5(2)(a) and 6.5(2)(b) do not apply, the disclosure will not be a contravention of the industry participant's obligations under the Privacy Act and the industry participant considers it appropriate to make such a disclosure.

(3) An industry participant must invite Australian law enforcement agencies to establish a memorandum of understanding or other cooperative agreement that:

(a) where the industry participant identifies end-user conduct or content on a dating service which the industry participant believes in good faith affords evidence of a serious and immediate threat to the life or physical safety of a person in Australia, the industry participant must as soon as practicable report the matter to a law enforcement authority (or otherwise as required by law);

(b) includes information on designated contact points in these agencies as well as the contact information described in section 6.5(1); and

(c) includes mechanisms for cooperation including the sharing of insights, trends or research findings on online safety issues, subject to any applicable privacy or data protection laws.

(4) If an agreement described in section 6.5(2) exists for an industry participant, whether this agreement is an agreement developed by the industry participant for its own purposes or this agreement has been developed by the code oversight body on a collective basis as set out in paragraph 2.1(1)(i) of Appendix A to this Code, the industry participant must implement appropriate systems, processes and policies to:

(a) allow for a risk-based assessment of each complaint (refer to section 6), possible incident detected by the dating service (refer to section 5.2(1)) or any other report received by the industry participant to determine if there is a risk of an imminent threat to the life or safety of the complainant or another directly impacted individual; and

(b) if there is a risk of an imminent threat to the life or safety of the complainant or another directly impacted individual, proactively escalate the complaint to the appropriate law enforcement agency in a timely manner in accordance with any established memorandum of understanding or other cooperative agreement.

Note: A threat to the life or safety of the complainant or another directly impacted individual can include a threat to their physical or mental health and safety. This can include a potentially life threatening situation or a situation which the dating service may consider to reasonably result in other serious injury or illness.

6.6 Reporting and referral obligations to other Australian Government agencies

Nothing in this Code supersedes an industry participant's existing referral or reporting obligations to Australian Government regulatory authorities (including eSafety) required under Australian law.

7 Trust and safety

7.1 Governance

(1) An industry participant must have a designated senior management employee who can carry out the following functions (the **Trust and Safety Leader**):

(a) promote a culture within the industry participant that proactively considers and deals with online safety issues related to the systems, processes and policies of the dating service;

(b) provide leadership within the industry participant on online safety matters; and

(c) regularly report to the industry participant's senior management on online safety issues related to the dating service.

(2) An industry participant must implement appropriate systems, processes and policies to provide clear oversight, accountability and lines of authority for all online safety decisions made by the industry participant including:

(a) if more than one team is responsible for online safety, appropriate arrangements to ensure these teams work together to address online safety issues; and

(b) implementing internal controls to enable the industry participant's progress on online safety issues to be measured.

(3) An industry participant must implement appropriate systems, processes and policies to collect meaningful data about the online enabled harm being experienced by Australian end-users which is aligned with the metrics for the reports required at sections 8.3 and 8.4 of this Code. The data collected should be readily accessible to the industry participant's trust and safety team.

7.2 Trust and safety teams

(1) An industry participant must have a trust and safety team which is sufficient to oversee the online safety systems, processes and policies for the dating service. The trust and safety team must have clearly defined roles and responsibilities, including for the creation, operationalisation and evaluation of the systems, processes and policies required under this Code.

(2) The industry participant must implement an adequate level of oversight and accountability by senior management (including the Trust and Safety Leader specified at section 7.1) over the functions and activities of the trust and safety team, and there should be clear protocols in place to enable online safety issues to be escalated within the industry participant.

(3) The industry participant may:

(a) allocate the roles and responsibilities of the trust and safety team to its employees or to external third-party service providers; or

(b) rely on the trust and safety team of a related body corporate to assist with complying with this obligation, provided such reliance does not compromise any party's compliance with this Code.

(4) An industry participant should ensure that its trust and safety team receives appropriate training to assist or refer end-users who have made a genuine complaint or report to the appropriate support (including the support resources specified in section 6.3).

7.3 **Informing end-users**

An industry participant must:

(1) provide Australian end-users with advice, resources and other supports about safe dating practices as part of its onboarding process for end-users, and in relevant direct communications with end-users;

Note: For example, individualised communications with end-users may include regular emails or notices to remind end-users of expectations on them in respect of an industry participant's online safety policies.

(2) ensure that information about the industry participant's:

(a) online safety policies;

(b) terms and conditions;

(c) community guidelines; and

(d) complaints and reports mechanism (refer to section 6.1),

are:

(e) regularly updated;

(f) easy to find by Australian end-users and provide clear and upfront expectations on acceptable conduct;

Note: For example, a dating service's online safety policies and terms and conditions may be held in a centralised location such as a regularly updated online resource hub.

(g) where reasonable, are written in any easy to understand manner such that they are comprehensible by a reasonable Australian consumer;

(h) meets the web accessibility standards established by the World Wide Web Consortium (**W3C**) including accessible formats for end-users with disability; and

(i) meets any other accessibility requirements appropriate for Australian end-users with disability considered by industry participants in consultation with relevant external stakeholders representing at-risk communities; and

Note: For example, accessible formats for end-users with disability include compatibility with screen readers and presenting content in a format which is easily understood by end-users with cognitive challenges. W3C web accessibility standards include the Web Content Accessibility Guidelines 2.0 or higher as detailed here: https://www.w3.org/TR/*.*

(3) proactively communicate with end-users about significant changes to its online safety policies (including through the use of targeted in-service communications).

7.4 **Industry collaboration and stakeholder engagement**

(1) Industry participants will collaborate with other participants (including law enforcement agencies, stakeholder groups and advisory bodies as appropriate) on the basis of the following guiding principles:

(a) Always learning – industry participants recognise that their systems, processes and policies must continuously improve to adapt to new and emerging technology and trust and safety issues.

(b) Open and transparent – industry participants will ensure their online safety practices are open and transparent to the Australian community.

(c) Shared responsibility – industry participants are equally responsible for ensuring the online dating environment is safe for the Australian community and will work together effectively to promote trust and safety best practice within the industry.

(2) An industry participant must participate in industry forums where practicable to:

(a) collaborate on trust and safety issues including key learnings and industry best practice initiatives;

(b) share intelligence on known and emerging online safety issues; and

(c) support smaller industry participants to improve their online safety systems, practices and policies to the extent reasonably possible (such as through the sharing of information in respect of technical solutions, processes or policies).

(3) The industry forums specified in paragraph 7.4(2) are to be held at least bi-annually and can be held in-person or virtually as determined by the code oversight body in consultation with industry participants. Law enforcement agencies and regulatory authorities (including eSafety) will be invited to attend these forums, and these forums will be arranged by the code oversight body.

(4) Industry participants may engage, through the code oversight body, with external stakeholder groups representing at-risk communities annually through roundtables or forums as appropriate to obtain feedback on the performance of this Code.

(5) The code oversight body will:

(a) at the request of industry participants, establish a memorandum of understanding or other cooperative agreement with appropriate external stakeholder groups and advisory bodies on a collective basis to ensure that stakeholder groups representing Australian end-users from at-risk communities are heard, and assist with evidence-based continuous improvement of online safety systems, processes and policies within the industry; and

(b) review any memorandum of understanding or other cooperative agreement established by the code oversight body on a regular and ongoing basis.

Note: For example, stakeholder groups include organisations representing at-risk communities.

8 Code administration

8.1 Commencement

(1) This Code will be adopted by industry participants on or before 30 June 2024.

(2) This Code will commence on 1 October 2024 (**Commencement Date**).

(3) A six-month transition period after the Commencement Date will apply to industry participants to allow for any changes to their systems, processes and policies to comply with this Code. Industry participants will not be subject to any enforcement action in relation to a contravention of a Code obligation or requirement during the transition period.

(4) Notwithstanding the transition period set out in section 8.1(3), industry participants will take reasonable steps to be able to publish the transparency reports required under section 8.4 as soon as practicable after the Commencement Date.

(5) eSafety will evaluate the effectiveness of this Code nine months after the Commencement Date.

8.2 Enforceability

(1) Industry participants agree that the code oversight body may make use of its enforcement powers, through an independent compliance committee established by the code oversight body and pursuant to the instrument which establishes such committee, against an industry participant which has contravened, or is contravening, this Code.

(2) Industry participants must keep records of the compliance measures they have adopted to comply with this Code for a period of 2 years.

8.3 Reporting to eSafety

(1) An industry participant must take reasonable steps to provide eSafety with updates, if it does not already do so, regarding significant changes to the functionality of its dating service which are likely to have a material positive or negative effect on the occurrence of online safety issues in respect of conduct by end-users. The industry participant may choose to provide this information in an annual report to eSafety.

(2) An industry participant must submit a Code report to eSafety which at a minimum contains the following information:

(a) the steps that the industry participant has taken to comply with the measures in this Code;

(b) the volume of complaints received by the industry participant which are handled in respect of section 6; and

(c) an explanation as to why the steps it has taken are in line with best practices and proportionate to the industry participant's size and maturity of the dating service.

(3) An industry participant must submit a Code report to eSafety as soon as practicable after 1 July 2025 and by no later than 31 August 2025, and on an annual basis thereafter, containing the information set out in section 8.3(2) for the

12-month period up to 30 June (inclusive) of the year in which the report is submitted to eSafety.

Note: Industry participants may not be able to obtain data for the full 12-month reporting period during the transition period. For the purposes of section 8.3(3), the relevant reporting period will be 1 April 2025 to 30 June 2025, although industry participants are encouraged to include data for periods prior to 1 April 2025 where reasonably possible.

8.4 **Reports to be published**

(1) An industry participant must publish a transparency report as soon as practicable after 1 July 2025 and by no later than 31 August 2025, and on an annual basis thereafter, which aligns with the Safety by Design principles and includes the following information (as a minimum) for the 12-month period up to 30 June (inclusive) of the year in which the report is published:

(a) the number of Australian end-users whose accounts have been terminated in accordance with section 5.4(2)(a) broken out by the policy basis for the termination;

(b) the number of instances where Australian end-user content has been moderated broken out by the mechanism for detection and enforcement;

(c) meaningful and comprehensible information about the content moderation engaged in at the industry participant's own initiative including:

(i) the use of automation technology;

(ii) measures taken to provide training and assistance to persons in charge of content moderation; and

(iii) the number and type of measures taken that affect the availability, visibility and accessibility of information provided by end-users and the end-user's ability to provide information through the dating service; and

(d) any use made of automation technology for the purpose of content moderation including a qualitative description, a specification of the purposes, indicators of the accuracy and possible rate of error of the automation technology used for these purposes.

Note: Industry participants may not be able to obtain data for the full 12-month reporting period during the transition period. For the purposes of section 8.4(1), the relevant reporting period will be 1 April 2025 to 30 June 2025, although industry participants are encouraged to include data for periods prior to 1 April 2025 where reasonably possible.

(2) For the avoidance of doubt, nothing in this Code requires the publication of information that would compromise the functionality or effectiveness of an industry participant's moderation practices, policies or technology.

8.5 **Code oversight body**

Industry participants must establish a code oversight body to assist with the administration and promotion of this Code to industry and the Australian community. The role of the code oversight body, as well as the bodies that the code oversight body may establish for the purpose of administering this Code, is set out at Appendix A. The bodies that may be established by the code oversight body include:

(1) an independent committee to review and decide on complaints submitted in respect of an industry participant's alleged contravention of the Code; and

(2) a secretariat to provide administrative and clerical support,

8.6 **Review**

(1) This Code will be reviewed by industry participants at the following points:

(a) two years after the Commencement Date; and

(b) at three-yearly intervals thereafter.

(2) Each review of this Code will be:

(a) coordinated by the code oversight body; and

(b) conducted in consultation with eSafety, industry participants and other interested stakeholders.

(3) Each review of this Code will consider as a minimum:

(a) how successful or unsuccessful this Code has been in preventing and mitigating online enabled harm among Australian end-users;

(b) the continued relevance of the compliance ratings for the dating service of each industry participant;

(c) any technological or other developments which have created gaps in this Code which should be filled, or which have rendered a compliance measure specified in this Code to be unnecessary;

(d) any technological or other developments which may impact the effective detection and handling of potential incidents of online enabled harm under this Code;

(e) aspects of this Code which have caused confusion for industry participants;

(f) how industry participants have complied with this Code, including results of any compliance monitoring and insights from complaints-handling (including areas of systemic non-compliance);

(g) public and stakeholder awareness, understanding and response to this Code; and

(h) any other matters raised by eSafety, law enforcement agencies or any other government agencies in relation to this Code.

(4) The industry working group or code oversight body which is responsible for conducting each review of this Code will:

(a) consult with eSafety on a confidential basis to prepare a draft revision to this Code;

(b) publish the draft revised Code for public consultation, and invite submissions from members of the public and any other stakeholders during a public consultation period that runs for at least 30 days;

(c) consider the submissions received during the public consultation period specified in section 8.6(4)(b);

(d) finalise the revision of this Code and submit the revised Code to eSafety for registration; and

(e) publish a summary of key issues raised in the submissions for the public consultation set out in section 8.6(4)(b).

Appendix A

Code oversight, administration and compliance

1 Definitions

1.1 In this Appendix, the following definitions apply unless the context otherwise requires:

(1) **Code** means the voluntary Code of Practice established by providers of dating services.

(2) **Code Compliance Committee** means the committee with the responsibilities set out in paragraph 3.1 of this Appendix.

(3) **Code Oversight Body** means the body with the responsibilities set out in paragraph 2.1 of this Appendix.

(4) **Code Register** means the official list of industry participants described in paragraph 2.1(1)(a) of this Appendix.

(5) **Code Secretariat** means the body with the responsibilities set out in paragraph 4.1 of this Appendix.

(6) **Code Website** means the website specified in paragraph 2.1(8) of this Appendix.

(7) **Information Request** means the information requested from an industry participant specified in paragraph 3.4(1) of this Appendix.

2 Code Oversight Body

2.1 Role of the Code Oversight Body

(1) The Code Oversight Body will be responsible for:

(a) maintaining a register of industry participants which are subject to the Code (**Code Register**);

(b) establishing and managing a process to include new organisations in the Code Register as industry participants which are subject to the Code

(c) establishing standards and criteria used for a dating service's self-assessment of their compliance rating under section 3.2 of the Code, and by the Code Compliance Committee to resolve disputes about a dating service's self-assessed compliance rating under paragraph 3.3 of this Appendix. The Code Oversight Body may choose to establish the standards and criteria in consultation with independent third party advice;

(d) establishing a list, developed in consultation with appropriate external stakeholder groups, of support resources for specific types of online enabled harm that industry participants should provide to Australian end-users for the purpose of section 6.3 of the Code;

(e) engaging law enforcement agencies and regulatory authorities (including eSafety) through bi-annual industry forums specified at section 7.4(2) of the Code;

(f) engaging external stakeholder groups on the industry's behalf, including through the external stakeholder forums specified at section 7.4(4) of the Code;

(g) regularly reviewing the Code in accordance with section 8.6 of the Code;

(h) assisting industry participants to promote the Code to the Australian community, including the preparation of material for educational purposes; and

(i) where applicable, developing memoranda of understanding or other cooperative arrangements relevant to the Code on a collective basis with:

(i) appropriate law enforcement authorities as set out in section 6.5 of the Code; or

(ii) external stakeholder groups and advisory bodies as set out in section 7.4(5) of the Code.

(2) The Code Oversight Body will engage with the Code Secretariat to establish and maintain a website which sets out the following minimum information (**Code Website**):

(a) governance arrangements for the Code including:

(i) oversight body and committee structures and terms of reference that set out how the Code Oversight Body, Code Compliance Committee, and the Code Secretariat will carry out their functions; and

(ii) Code Compliance Committee member biographies and any other material that the Code Compliance Committee considers to be relevant and appropriate for publication on the Code Website;

(b) the verified compliance ratings of industry participants pursuant to section 3.2(3) of the Code;

(c) published reports including the transparency report required under section 8.4 of the Code; and

(d) how a person may make a complaint to the Code Compliance Committee about an industry participant's alleged contravention of the Code.

(3) Where applicable, the Code Oversight Body will engage with the Code Secretariat to:

(a) review and update the terms of reference described in paragraph 2.1(2)(a)(i) of this Appendix; and

(b) establish, review and update guidelines for one or more activities undertaken by the Code Oversight Body, Code Compliance Committee or the Code Secretariat.

(4) The Code Oversight Body's activities on behalf of industry participants for the purposes of the Code will not be to the exclusion of the activities of individual industry participants on online safety.

2.2 Membership of the Code Oversight Body

(1) Each industry participant will nominate a representative to be a member of the Code Oversight Body. Industry participants can change their nominated representative at any time by providing written notice to the Code Secretariat.

(2) The Code Secretariat will within a reasonable period notify the following Australian Government agencies of changes to the representatives:

(a) eSafety; and

(b) the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

3 Code Compliance Committee

3.1 Role of the Code Compliance Committee

(1) The Code Compliance Committee is an independent committee established by industry participants to:

(a) resolve complaints submitted to the Code Compliance Committee through the complaints mechanism available on the Code Website about an industry participant's contravention or alleged contravention of the Code in accordance with the committee's terms of reference;

(b) review and either confirm or reject a dating service's self-assessed compliance rating as set out in section 3.2 of the Code. If the Code Compliance Committee rejects a dating service's self-assessment of their compliance rating, the committee must provide that industry participant with:

(i) a revised compliance rating which aligns with the standards and criteria set out in paragraph 2.1(1)(c) of this Appendix;

(ii) detailed reasons as to why the committee does not agree with the dating service's self-assessed compliance rating; and

(iii) if the committee considers this to be applicable, the steps which the dating service must take (and as verified by the committee) in order for the self-assessed compliance rating to apply to the dating service; and

(c) resolve disputes submitted to the Code Secretariat by an industry participant about a dating service's compliance rating as set out in section 3.2 of the Code.

(2) The Code Compliance Committee must comply with the terms of reference and any guidelines issued by the Code Oversight Body when performing its duties as set out in paragraph 3.1(1) of this Appendix.

3.2 Complaints handling

(1) The Code Compliance Committee can review and resolve complaints submitted in respect of an industry participant's alleged contravention of the Code which:

(a) have been submitted through the Code Website complaints mechanism; and

(b) relate only to the industry participant's contravention or an alleged contravention of the Code.

Note: For example, the Code Compliance Committee cannot review a complaint submitted by a complainant about another end-user's conduct which violates an industry participant's online safety policies, such as alleged sexual misconduct. However, the complainant may submit a complaint to the Code Compliance Committee if the industry participant concerned did not notify the complainant about the outcome of the industry participant's investigation of the initial sexual misconduct complaint as required under section 6.2(1)(c) of the Code.

(2) For the avoidance of doubt, the Code Compliance Committee must not:

(a) review a complaint made solely about another end-user's contravention or alleged contravention of an industry participant's online safety policies. Complaints of this nature must be submitted to, and be resolved by, the relevant industry participant; or

(b) review the merits of any decision made by an industry participant about a complaint which the complainant previously submitted to the industry participant about another end-user's contravention or alleged contravention of that industry participant's online safety policies.

3.3 Disputes handling

(1) The Code Compliance Committee can review and resolve disputes which have been submitted through the Code Secretariat by an industry participant concerning the accuracy of another dating service's compliance rating as set out in section 3.2 of the Code.

(2) The Code Compliance Committee's decision on the compliance rating of a dating service shall be final.

3.4 Membership of the Code Compliance Committee

(1) The Code Compliance Committee will be made up of three independent members selected by a majority of the Code Oversight Body based on the following criteria:

(a) one member must be legally qualified and admitted to practice as a solicitor in an Australian jurisdiction;

(b) one member must have relevant experience in matters relating to public policy, public administration, online safety or sexual or gender based violence; and

(c) one member must have relevant experience in large-scale, social networking technology platforms.

(2) Members of the Code Compliance Committee:

(a) will be appointed for a term of 12 months in accordance with the committee's terms of reference;

(b) must not be an employee of an industry participant at any time during their appointment as a member of the committee; and

(c) must declare any actual or potential conflict of interest as a condition of their appointment.

(3) There will be no limit on the number of terms that a member of the Code Compliance Committee may be appointed for.

(4) The Code Oversight Body may pass a resolution to remove a person from their position on the Code Compliance Committee in accordance with any procedural guidelines on the grounds set out in the committee's terms of reference.

3.5 Code Compliance Committee meetings

(1) The Code Compliance Committee will meet on a quarterly basis to:

(a) review and resolve complaints about an industry participant's contravention or alleged contravention of the Code; and

(b) take any one or more of the steps set out in paragraph 3.5 of this Appendix including to determine whether a non-compliant industry participant has complied with a rectification or remediation order.

(2) The Code Secretariat may provide advice and recommendations to the Code Compliance Committee regarding the operation of this Code and will record minutes of committee meetings and assist in documenting the committee's decisions and reports.

(3) The Code Compliance Committee may choose to conduct a meeting outside of the scheduled quarterly meetings if:

(a) all committee members are unable to attend a scheduled quarterly meeting;

(b) the committee unanimously considers an out-of-session meeting to be necessary due to urgent circumstance; or

(c) the Code Secretariat has determined that more than one meeting is required for the committee to review and resolve the complaints at hand, and the committee agrees with the Code Secretariat's recommendation for additional meetings to be held.

3.6 Requesting information from industry participants

(1) The Code Secretariat may request, on the Code Compliance Committee's behalf, that industry participants provide information and records that relate to a complaint which falls within the committee's jurisdiction (**Information Request**).

(2) Industry participants must comply with an Information Request unless such compliance would cause the industry participant to breach any other obligation under Australian law (including obligations of privacy and confidentiality).

(3) If an industry participant cannot comply with an Information Request, the industry participant must provide the Code Compliance Committee, through the Code Secretariat, with reasons why they cannot comply (including any applicable Australian law which prohibits them from complying with the Information Request).

3.7 Sanctions on non-complying industry participants

(1) The Code Compliance Committee can impose any of the following sanctions on industry participants found to have contravened the Code:

(a) **formal warning:** the Code Compliance Committee may issue a formal warning to the non-compliant industry participant. If the industry participant continues to be non-compliant, the Code Compliance Committee may subject the industry participant to any other sanction which it deems appropriate based on the nature of the contravention and/or the industry participant's history of non-compliance with the Code;

(b) **remediation order:** the Code Compliance Committee may require a non-compliant industry participant to enter into a remediation plan which sets out the steps that the industry participant will take over a specified timeframe to address one or more contraventions of the Code, including any review of the industry participant's systems, processes and policies where appropriate. The industry participant must:

(i) prepare the remediation plan, and provide the remediation plan to the committee for approval;

(ii) if the remediation plan is approved by the committee (including approvals which are subject to conditions or amendments required by the committee), comply with the remediation plan; and

(iii) provide the committee with a summary report on the steps which the industry participant has taken to comply with the remediation plan;

(c) **suspension from the Code:** the Code Compliance Committee may:

(i) suspend a non-compliant industry participant's certification as being compliant with this Code; and

(ii) require the industry participant to cease portraying itself as compliant with this Code, including prohibiting the use of any accreditations, labels or references to its compliance with this Code in any marketing or online material published by the industry participant,

if:

(iii) the industry participant has not satisfied any obligation imposed by the committee in previous sanctions; and

(iv) the committee determines that the industry participant's suspension is appropriate based on their history of past contraventions;

(d) **removal from the Code:** the Code Compliance Committee may remove the non-compliant industry participant as a signatory to the Code if:

(i) the industry participant has not satisfied any obligation imposed by the committee in previous sanctions; and

(ii) the committee determines that the industry participant's removal from the Code is appropriate based on their history of past contraventions.

(2) An industry participant may apply to the Code Compliance Committee for a reconsideration of a decision imposing a sanction on that industry participant. The committee will only consider applications which are supported by new evidence provided by the industry participant.

(3) The Code Compliance Committee may impose a formal warning or remediation order on an industry participant on an interim basis for a period of time determined by the committee, if the committee considers the application of an interim sanction to be appropriate in the circumstances.

Note: For example, the Code Compliance Committee considers an industry participant has demonstrated it was acting in good faith in its efforts to comply with the Code despite the contravention.

(4) The Code Compliance Committee must publish the following information on the Code Website:

(a) the name of an industry participant who is subject to an ongoing remediation order (other than an interim remediation order);

(b) the name of an industry participant who has been suspended from the Code and the suspension remains current; and

(c) the name of an industry participant who has been removed as a signatory to the Code and the date they re-joined as a signatory to the Code (if applicable).

4 Code Secretariat

4.1 Role of the Code Secretariat

(1) Industry participants will establish the Code Secretariat to provide administrative and clerical support to the Code Oversight Body and the Code Compliance Committee.

(2) The Code Secretariat will undertake the following functions:

(a) advise the relevant committees on procedures and practice in accordance with the relevant terms of reference;

(b) assess whether complaints received through the complaints mechanism on the Code Website are complaints that fall under the jurisdiction of the Code Compliance Committee as set out in paragraph 3.1(1)(a) of this Appendix.

(c) prepare agenda items and other material for committee meetings and record all meeting outcomes;

(d) prepare briefs to members setting out the complaints to be resolved at Code Compliance Committee meetings including any background material provided by industry participants who are the subject of the complaints;

(e) request information from industry participants on behalf of the Code Compliance Committee under paragraph 3.6(1) of this Appendix;

(f) maintain and update the Code Website as directed by the Code Oversight Body; and

(g) provide any other administrative and clerical support that may be required by the Code Oversight Body or the Code Compliance Committee.