

Trusted eSafety Provider Agreement

Commonwealth of Australia represented
by the eSafety Commissioner



Contents

Parties	3
Purpose of the Program.....	4
Purpose of this Agreement	4
Scope of this Agreement.....	5
Commencement, variation and termination	5
Insurance coverage, compliance, child safety	6
Workers.....	7
Program content	7
Intellectual property	8
Program branding, promotion and online content	8
Community of practice	9
Program assurance and reporting	9
Handling of complaints and potential breaches	10
Liability and indemnity.....	10
Survival.....	11
Notices	11
General.....	11
Definitions.....	12
Schedule 1 – Copy of Submitted Trusted eSafety Provider Program Application.....	14
Schedule 2 – Community of practice	15
Schedule 3 – Program branding and promotion	17
Schedule 4 – Annual reporting requirements.....	21
Schedule 5 – Processes for handling complaints and breaches	22
Execution page.....	26

Parties

THE COMMONWEALTH OF AUSTRALIA ('the Commonwealth') represented by the eSafety Commissioner; ABN 12 212 931 598 of Red Building, Benjamin Offices, Chan Street, Belconnen, ACT, 2616 ('us', 'we', 'our', 'the Commissioner' or 'eSafety' as the case requires).

AND

[Insert business name and ABN/ACN] of [insert address] as the Trusted eSafety Provider ('you', 'your' or 'your organisation' as the case requires).

Reference Schedule

Details of Trusted eSafety Provider	
Full legal name of Trusted eSafety Provider	{{applicant__companyname}}
Trading or business name	{{applicant__esafety_tradingname}}
Australian Company Number (ACN) or other entity identifiers	{{applicant__esafety_acn}}
Australian Business Number (ABN)	{{applicant__esafety_abn}}
Authorised Officer	{{ceo__fullname}}
Registered office (physical/postal)	{{applicant__address1_line1}} {{applicant__address1_line2}} {{applicant__address1_city}} {{applicant__esafety_address1_state}} {{applicant__address1_postalcode}} {{applicant__address1_country}}
Authorised officer telephone	{{ceo__telephone1}}
Authorised officer email address	{{ceo__emailaddress1}}
eSafety Details	
Name	The Commonwealth of Australia represented by the eSafety Commissioner
Australian Business Number (ABN)	12 212 931 598
Authorised Officer	Manager, Grants and Education Providers
Address	Benjamin Offices, Red Building Level 4 Chan Street BELCONNEN ACT 2615.
Email address	trustedproviders@esafety.gov.au

Purpose of the Program

Context

The eSafety Commissioner (eSafety) administers the Trusted eSafety Provider Program (the Program) on behalf of the Commonwealth in accordance with the Commissioner's legislative functions, as specified at section 27(1)(f) of the *Online Safety Act 2021*.

Under the Program, eSafety may endorse online safety education providers as a 'Trusted eSafety Provider' (Provider) where they have demonstrated relevant expertise, an evidence-based approach and compliance with appropriate child safety, insurance and other relevant requirements.

To be eligible for endorsement, providers must offer one or more programs that are primarily and explicitly concerned with educating Australians and increasing their capacity to use social media services, electronic services and designated internet services in a safe manner (an 'Online Safety Education Program').

To maintain endorsement, a Provider must participate in a community of practice, report key information to eSafety annually, and comply with this Trusted eSafety Provider Agreement (the Agreement).

Providers are recognised as leaders in the development and delivery of online safety education who are also committed to the highest standards of professionalism and child safety.

eSafety encourages schools and other organisations seeking an online safety education provider to use a Trusted eSafety Provider.

Aims

The Program supports eSafety's mission to 'help safeguard Australians at risk from online harms and to promote safer, more positive online experiences'¹.

The aims of the Program are to:

- help schools and other organisations to identify and confidently select a suitable online safety education provider;
- promote best practice, evidence-based approaches to the development and delivery of online safety education; and
- raise awareness and understanding among children, young people, teachers, parents and other Australians of how eSafety can help them.

Purpose of this Agreement

1. This Agreement sets out the terms and conditions of your endorsement as a Trusted eSafety Provider.
2. This Agreement also sets out eSafety's commitments under the Program.
3. By entering into this Agreement, you acknowledge and agree that you have read and accepted the terms and conditions of this Agreement in full.

¹ Australia's eSafety Strategy 2022-2025

Scope of this Agreement

4. This Agreement contains the entire agreement and understanding between the parties on everything connected with this Agreement and supersedes any prior agreement or understanding on anything so connected.
5. This Agreement comprises:
 - a) this document;
 - b) the attached Schedules; and
 - c) any other document referenced or incorporated in this Agreement.

If there is any ambiguity or inconsistency between the documents comprising this Agreement, the document appearing higher in the above list will take precedence to the extent of any ambiguity or inconsistency.

Commencement, variation and termination

6. This Agreement commences on the Commencement Date and terminates on the Expiry Date unless it is terminated earlier in accordance with the provisions herein.
7. eSafety may vary this Agreement by giving you notice of the variation to this Agreement (Variation Notice). If you do not agree with the variation to this Agreement as set out in the Variation Notice, you may terminate this Agreement by giving eSafety 21 calendar days' written notice of your intention to terminate this Agreement in accordance with this clause 7. You will be taken to have accepted the variation to this Agreement as set out in the Variation Notice if you do not respond in writing to the Variation Notice within 21 calendar days from the date of the Notice.
8. eSafety may offer to extend the duration of this Agreement by giving you written notice of any extension. Any extension may be subject to you providing specified information or meeting such other conditions as specified in a notice that may be given to you under this clause.
9. eSafety may terminate this Agreement at any time, giving notice:
 - a) where you do not comply with this Agreement;
 - b) where significant changes occur in relation to any aspect of your activities, operations or ownership, as described in the information you provided for your application, which make you ineligible for endorsement under this Agreement; or
 - c) at the discretion of eSafety.
10. You may terminate this Agreement at any time by giving us no less than 30 calendar days' written notice.
11. If either party exercises its termination rights under this Agreement, the termination will not prejudice the rights or claims of either party in existence prior to that termination.
12. Upon termination or expiry of this Agreement, you must immediately:
 - a) cease to use the logo and branding and any other insignia specified in Schedule 3;
 - b) cease to represent that you are a Trusted eSafety Provider; and
 - c) remove all references to your affiliation with eSafety including in all your program and promotional material.

Insurance coverage, compliance, child safety

13. You agree to maintain insurance coverage appropriate for your organisation including:
- a) public liability insurance of at least 10 million dollars per annum (unless your liability is limited by virtue of membership of a scheme approved under Professional Standards Legislation in the relevant state, in which case the amount required by that scheme);
 - b) professional indemnity insurance of at least five million dollars per annum (unless your liability is limited by virtue of membership of a scheme approved under Professional Standards Legislation in the relevant state, in which case the amount required by that scheme); and
 - c) workers' compensation insurance if applicable (for an amount required by the applicable law).
14. You warrant that:
- a) all relevant Workers in your organisation who are required by law to have a Working with Children Check (or equivalent) in order to undertake their duties under this Agreement do so in accordance with the requirements of each jurisdiction in which they work (which may extend to scenarios where work involves electronic communication with children in another jurisdiction);
 - b) you have a child safety policy in place that:
 - i) addresses applicable legal requirements regarding mandatory reporting of suspected child abuse or neglect for each jurisdiction in which you deliver Online Safety Education Program(s);
 - ii) aligns with the National Principles for Child Safe Organisations or equivalent State or Territory standards;
 - iii) is reviewed annually and updated where required; and
 - iv) you will make available to each of your Clients,
 - c) you will request relevant information from each Client in relation to their own child safety policies and procedures.
15. When dealing with Personal Information, you agree:
- a) to comply with the requirements of the *Privacy Act 1988 (Cth)*;
 - b) not to do anything which, if done by the Commonwealth, would be a breach of an Australian Privacy Principle under the *Privacy Act 1988 (Cth)*;
 - c) to ensure that any Workers who deal with Personal Information for the purposes of this Agreement are aware of the requirements of the *Privacy Act 1988 (Cth)* and your obligations under this clause; and
 - d) to immediately notify us if you become aware of an actual or possible breach of this clause by you or any of your Workers and, if required under Privacy Laws, you must report this breach to the Office of the Australian Information Commissioner.
16. Certain information contained in or provided under this Agreement may be used for public reporting purposes subject always to our obligations under the *Online Safety Act 2021 (Cth)* and the *Privacy Act 1988 (Cth)*.

Workers

17. You warrant that all of your current and future Workers:

- a) have the necessary knowledge and skills to deliver your organisation's Online Safety Education Program(s). This may be through formal qualifications, relevant prior experience and/or your induction, training or professional development programs;
- b) have access to regular feedback and professional development to maintain and further develop relevant knowledge and skills;
- c) comply with relevant child safety standards in relation to appropriate communication, touch and interactions (including not being alone with children) and showing appropriate behaviour at all times;
- d) comply with your organisation's child safety policy, including processes to manage and respond to a disclosure of harm or abuse, or potential harm or abuse;
- e) comply with relevant Commonwealth and state and territory mandatory reporting requirements for reporting suspected child abuse and neglect, and other legal requirements for each jurisdiction in which you operate; and
- f) have access to appropriate support to manage their mental health and wellbeing.

Program content

18. Your endorsed program(s) must:

- a) be primarily and explicitly concerned with increasing the capacity of the audience to use social media services, electronic services and designated internet services in a safe manner and avoid a range of online harms (an 'Online Safety Education Program').
- b) raise awareness of eSafety, including by:
 - i. providing specific information about eSafety's regulatory and reporting schemes (for example, the cyberbullying, image-based abuse, adult cyber abuse, illegal and restricted online content schemes) as relevant to the program and audience;
 - ii. informing Online Safety Education Program participants that the eSafety website ([eSafety.gov.au](https://www.esafety.gov.au)) provides a range of information and resources for various audiences; and
 - iii. including any mandatory materials provided by eSafety and addressing any additional mandatory topics as otherwise determined by eSafety and notified to you in writing.

19. Your Online Safety Education Program(s) and professional conduct must align with the five elements of eSafety's Best Practice Framework for Online Safety Education, and the effective practices as applicable.

20. Your Online Safety Education Program(s) must not:

- a) include partisan political views or partisan political advocacy;
- b) advocate or proselytise for a religious view; or
- c) recommend, endorse or otherwise promote any online safety providers, products or services where you have an **undisclosed** commercial relationship with a supplier of those products or services – including but not limited to receiving sales commission, sponsorship, endorsement or any other benefit.

21. You agree to regularly review your Online Safety Education Program(s) and update where necessary to ensure it remains consistent with relevant best-practice and research, and relevant changes in technology, legislation and school curricula.

Intellectual property

22. You warrant that any materials used in your Online Safety Education Program(s) will not breach another person's intellectual property rights, including eSafety's rights.
23. You agree to the following requirements in relation to the use of materials provided by eSafety (eSafety Materials):
- a) Unless otherwise advised, eSafety materials are published under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence with the exception of materials identified at <https://www.esafety.gov.au/about-us/corporate-documents/disclaimer-copyright>.
 - b) We may provide you with eSafety materials on the basis that you do not distribute them to any third parties. Failure to comply with instructions from eSafety in relation to the handling and/or distribution of eSafety materials may constitute a breach of this Agreement and may lead to further compliance and enforcement action.
24. eSafety agrees that any material provided by you under this Agreement will be used in accordance with the terms of this Agreement and only for the purposes of performing its obligations and exercising its rights under this Agreement.

Program branding, promotion and online content

25. The Parties agree that they will raise awareness and understanding of the Program among schools and other potential audiences in accordance with Schedule 3.
26. You agree to the following in relation to the promotion and branding of your endorsement status:
- a) your endorsement under this Agreement applies only to the parts of your education program(s) that relate to online safety, which means that it does not extend to other parts of your education program(s) or any other activities, services or products that your organisation delivers;
 - b) representation of your endorsement under the Program must only be described as 'Trusted eSafety Provider' and must be consistent with the branding and promotion guidelines at Schedule 3;
 - c) your endorsement must not be used in any way that may imply that you are an employee, agent or contractor of eSafety or affiliated with eSafety in any other capacity than as a Trusted eSafety Provider.
27. Where you expressly identify yourself as a provider of Online Safety Education Programs online, including on your professional website, blog or social media accounts, you must use your best endeavours to ensure that the content you post or share online does not bring the reputation or standing of eSafety, the Program, or other Providers into disrepute.

28. If eSafety determines, in its absolute discretion, that content posted or shared to your website, blog or social media account is likely to bring the reputation or standing of eSafety, the Program, or other Providers into disrepute, eSafety may, by written notice:
- a) request that you remove specified content; and
 - b) investigate the content specified in the notice given to you under this clause 28 as a potential breach of this Agreement in accordance with clause 40 and Schedule 5.

Community of practice

29. eSafety will operate a community of practice for the Program to facilitate collaboration, share research and best practice, and promote continuous professional development and improvement. Terms of reference for the community of practice are contained in Schedule 2 of this Agreement.
30. The Parties acknowledge a shared responsibility to participate in and contribute to the effective operation of the Trusted eSafety Provider community of practice.
31. You agree that at least one representative from your organisation will attend at least two of the three general sessions each financial year. This representative must have sound knowledge of and influence over your Online Safety Education Program(s).
32. You agree that you are responsible for your representative(s) participating fully in the Trusted eSafety Provider community of practice in accordance with Schedule 2.

Program assurance and reporting

33. You agree to report annually to eSafety each financial year in which this Agreement operates. Annual reporting requirements are outlined at Schedule 4 of this Agreement.
34. You agree to inform each Client that they can provide feedback or register a complaint to eSafety about your Online Safety Education Program(s) through the Trusted eSafety Provider Feedback Portal on the eSafety website ([eSafety.gov.au](https://www.esafety.gov.au)). You agree to provide each school or other Client with the link to the Feedback Portal for the purposes set out in this clause 34.
35. eSafety will only share feedback received through the Feedback Portal with the Provider to which the feedback relates, subject to:
- a) eSafety obtaining the prior consent of the Client to do so; and
 - b) our obligations under Privacy Laws.
36. eSafety will handle complaints received through the Feedback Portal in accordance with this Agreement (see clauses 40–43 and Schedule 5).
37. You acknowledge and agree that eSafety will periodically audit your compliance with this Agreement, which may involve us:
- a) observing delivery of your Online Safety Education Program(s);
 - b) requesting feedback from one or more of your recent Clients; and
 - c) reviewing specified information and documents referenced in this Agreement.
38. You agree to cooperate with any requests from eSafety to facilitate an audit or carry out any other compliance activities in accordance with its legislative functions under the *Online Safety Act 2021* (Cth).

39. You agree to advise eSafety of any significant change to your organisation within 21 calendar days, including:
- a) information about significant changes to its ownership;
 - b) changes to the business or operating name;
 - c) changes to the Authorised Officer, mailing or contact address, including website and email domains;
 - d) changes to your registration as Australian Business (ABN) or an Australian Company (ACN), including any changes to your ABN or ACN; and
 - e) any other change that may affect your eligibility to be endorsed under this agreement.

Handling of complaints and potential breaches

40. You acknowledge that eSafety is authorised and obliged to investigate potential breaches of this Agreement arising from a complaint or other source of information.
41. eSafety will investigate a complaint received about a Provider in accordance with the principles set out in the eSafety Complaint Handling Policy.
42. The process by which eSafety will investigate complaints and potential breaches of this Agreement is set out in Part 1 of Schedule 5 of this Agreement.
43. If an investigation under this clause establishes that the Provider failed to uphold expected standards of professional and ethical conduct, or breached one or more terms of this Agreement, the process by which eSafety will respond to such breach is set out in Part 2 of Schedule 5.

Liability and indemnity

44. You agree to indemnify us from and against any:
- a) cost or liability incurred by us;
 - b) loss of or damage to our property (including Intellectual Property Rights); or
 - c) loss or expense incurred by us in dealing with any claim against us including legal costs and expenses on a solicitor/own client basis and the cost of time spent, resources used or disbursements paid by us, arising from:
 - i) any breach by you of this Agreement;
 - ii) any act or omission involving fault by you in connection with this Agreement; or
 - iii) any allegation of any infringement of any intellectual property rights.
45. Your liability to indemnify us under this clause will be reduced proportionately to the extent that our negligent act or omission directly contributed to the relevant cost, liability, loss, damage or expense.
46. Our right to be indemnified under this clause is in addition to, and not exclusive of, any other right, power or remedy provided by law, but we are not entitled to be compensated in excess of the amount of the relevant cost, liability, loss, damage or expense.
47. You release us from any liability to you in respect of your representations regarding your Trusted eSafety Provider status.

Survival

48. The following provisions survive termination or expiry of this this Agreement:

- a) clause 12;
- b) clause 15;
- c) clause 17(c);
- d) clause 17(d); and
- e) clause 17(e).

Notices

49. A notice under this Agreement must be in writing and will be deemed to be effected:

- a) if delivered by hand – upon delivery to the relevant address;
- b) if sent by prepaid post – on the day which is 3 Working Days after posting; and
- c) if transmitted by email – on the day of sending.

A notice received after 5.00 pm, or on a day that is not a Working Day in the place of receipt, is deemed to be effected on the next Working Day in that place.

General

50. In the interpretation of this Agreement, unless the context otherwise requires:

- a) words importing the singular will include the plural and vice versa;
- b) clause headings will be disregarded; and
- c) all warranties will, during the term of this Agreement, have the force and effect of conditions, and survive termination or expiry of this Agreement.

Definitions

In this Agreement, unless the contrary appears:

- **Agreement** means the Trusted eSafety Provider Agreement, Schedules and any other document referenced or incorporated in the Agreement document.
- **Child** refers to anyone under the age of 18, consistent with the United Nation's Convention on the Rights of the Children and the *Family Law Act 1975* (Cth).
- **Client** means a person or organisation that engages a Trusted eSafety Provider to deliver an Online Safety Education Program(s).
- **Commencement date** means the date this Agreement is executed (countersigned) by the eSafety Commissioner or their delegate.
- **Commonwealth** means the Commonwealth of Australia as represented by the eSafety Commissioner.
- **Complaint** refers to an expression of dissatisfaction made to or about an organisation, related to its services, the conduct of its employees or the handling of an earlier complaint.
- **Effective practices** refers to the 22 effective practices included in the eSafety's [Best Practice Framework](#) for online safety education.
- **Elements** refers to the five elements of eSafety's [Best Practice Framework](#) for online safety education.
- **Expiry date** means the date that is 24 months from the Commencement Date.
- **Feedback Portal** means the form by which Clients of Providers can provide feedback to eSafety, located on the eSafety website, currently at <https://www.esafety.gov.au/educators/trusted-providers/feedback>.
- **Harm** refers to significant detriment to a child's physical, psychological or emotional wellbeing or emotional development. Harm may be caused by physical, psychological, or emotional abuse or neglect, sexual abuse or other exploitation, or exposure to physical violence.
- **Intellectual Property Rights** means all copyright, patents, registered and unregistered trademarks (including service marks), registered designs, and other rights resulting from intellectual activity (other than moral rights under the *Copyright Act 1968*).
- **Mandatory reporters/Mandatory reporting legislation** generally contains lists of particular occupations that are mandated to report cases of suspected child abuse and neglect. The groups of people mandated to report range from persons in a limited number of occupations (QLD) to a more extensive list (VIC and WA), to a very extensive list (ACT, NSW, SA and TAS), through to every adult (NT). The occupations most commonly named as mandated reporters are those who deal frequently with children in the course of their work: teachers, early childhood education and care practitioners, doctors, nurses and police.

- **National Principles for Child Safe Organisations** refers to the 10 principles of the [National Principles for Child Safe Organisations](#) published by the Australian Government.
- **Online Safety Education Program** refers to educational programs and related content that are primarily and explicitly concerned with educating Australians and increasing their capacity to use social media services, electronic services and designated internet services in a safe manner.
- **Party** means the applicant/s or the Commonwealth.
- **Personal information** has the same meaning given to it in section 6 of the *Privacy Act 1988* (Cth). 'Information or an opinion about an identified individual, or an individual who is reasonably identifiable:
 - a) whether the information or opinion is true or not; and
 - b) whether the information or opinion is recorded in a material form or not.'
- **Privacy Laws** refers to the *Privacy Act 1988* (Cth) and any other Act or other legislative instrument requiring privacy, secrecy, or confidentiality in dealing with information.
- **Program** means the Trusted eSafety Provider Program.
- **Provider** means Trusted eSafety Provider.
- **Term** means the period commencing on the Commencement Date and expiring on the Expiry Date, subject to any variation or extension as agreed between the parties.
- **Worker** has the same meaning as in section 7 of the *Workplace Health and Safety Act 2011*. A person is a worker if the person carries out work in any capacity for a person conducting a business or undertaking, including work as an employee, a contractor or subcontractor, an employee of a contractor or subcontractor, an employee of a labour hire company who has been assigned to work in the person's business or undertaking, an outworker, an apprentice or trainee, a student gaining work experience, a volunteer or a person of a prescribed class. In this Agreement, the definition of 'Worker' includes any employees of the Trusted eSafety Provider during the term of this Agreement.
- **Working Day** means each day except Saturdays, Sundays and public holidays.
- **Working With Children Check (WWCC)** refers to an assessment of whether a person poses an unacceptable risk to children. As part of this process, the applicant's criminal history, child protection information and other information is checked. A WWCC may also be known by other names, including Working with Vulnerable People(WWVP), a Blue Card, Working with Children Clearance, or Ochre Card.

Schedule 1 – Copy of submitted Trusted eSafety Provider Program application

[Copy of all information submitted in application]

Schedule 2 – Community of practice

Purpose

The community of practice is a forum to promote best-practice in online safety education and facilitate sharing and collaboration between eSafety and Providers, and among Providers, consistent with the aims of the Program.

eSafety and Providers are committed to engaging cooperatively and collaboratively through the community of practice to advance the shared goal of promoting safer, more positive online experiences for Australian students and the broader community.

The value of the community of practice is greatest when all members actively participate, combining their diverse experience and expertise to support mutual professional development and continuous improvement of programs and services.

Membership

All currently endorsed Trusted eSafety Providers are members of the community of practice, together with relevant eSafety staff.

Providers are asked to nominate a primary contact for the community of practice, however, additional or alternate representatives may participate as necessary or appropriate. Representatives must have sound knowledge of and influence over the Provider's Online Safety Education Program(s).

Membership of any sub-group that may be established under the community of practice will be on an opt-in basis.

Format

General meetings

eSafety will convene three general meetings of the community of practice each financial year. These sessions will be approximately two hours long and will typically be held online during school holidays to enable as many Providers to attend as possible. Face-to-face sessions may be considered subject to interest.

General meetings will be structured to support information sharing, professional learning and collaboration through items such as guest presenters (from eSafety, Providers, and external organisations), topic deep-dives, research translations, and sharing emerging issues and insights. General meetings also provide an opportunity for eSafety and Providers to discuss any issues regarding the Program.

Providers are encouraged to play an active role in proposing, leading and contributing to items at these meetings.

Other engagement

The community of practice can facilitate additional opportunities for engagement with and between Providers, based on interests and demand. eSafety will develop these in consultation with Providers but may include, for example:

- working groups on particular issues (e.g. to develop a shared resource)
- shorter sessions addressing a single topic of interest or urgency
- online information sharing and collaboration
- email / electronic newsletter.

Roles and responsibilities

eSafety commits to:

- consult with Providers on the timing of general meetings and confirm meeting dates and times at the start of each year
- create opportunities for Providers to shape the community of practice, including through nominating priorities and contributing to the planning of activities throughout the year
- facilitate two-way sharing of operational insights between Providers and eSafety (e.g. relevant trends in reports to eSafety, emerging online safety issues in schools)
- create opportunities for Providers to engage with each other
- create opportunities for Providers to initiate and lead activities – individually or with other Providers
- organise relevant eSafety and external guest speakers to feature in sessions
- circulate papers at least one week before each general meeting and a summary including relevant documents and links after each general meeting, and
- chair meetings as required (Providers may also nominate to do this).

Each Provider commits to:

- attendance at a minimum of two general meetings each financial year (in accordance with clause 31)
- reviewing communications and meeting papers
- actively participating in community of practice sessions
- engaging positively and respectfully with other members in a collegiate manner, and
- exercise discretion and where required maintaining confidentiality in relation to information shared within the community (see also clause 23. b) with respect to specified eSafety materials).

Providers are also encouraged to:

- help set the direction and priorities for the community of practice including by proposing relevant topics and guest speakers, and
- contribute to the operation of the community of practice by leading or helping to facilitate session items or other initiatives including development of shared resources.

Schedule 3 – Program branding and promotion

Purpose

Building awareness and understanding of the Trusted eSafety Provider Program among schools and other target audiences is critical to its success.

Consistent and prominent promotion by Providers of their endorsement complements eSafety’s promotion of the Program, helping schools and other audiences recognise and value the Trusted eSafety Provider brand.

The following guidelines establish requirements for Providers when representing their endorsement and outline how the parties will work together to promote the Program.

Written representation of affiliation with eSafety

1. The following standard description of endorsement should be used wherever possible:

“[Organisation name] is endorsed by the eSafety Commissioner as a Trusted eSafety Provider.”

2. Wherever possible, this should be accompanied by a link to the relevant page on the eSafety website to enable the reader to learn what the endorsement means. This may be done as follows:

“[Organisation name] is endorsed by the eSafety Commissioner as a [Trusted eSafety Provider](https://www.esafety.gov.au/educators/trusted-providers/).”

[link: <https://www.esafety.gov.au/educators/trusted-providers/>]

or

“[Organisation name] is endorsed by the eSafety Commissioner as a Trusted eSafety Provider. To learn more visit [esafety.gov.au/trusted-providers](https://www.esafety.gov.au/trusted-providers/).”

3. Providers may describe their endorsement using different phrasing to the examples above as appropriate to the context, however, all written representations of endorsement must observe the language requirements below:

Reference	Compliant	Not compliant (examples)
Endorsed entity	Trusted eSafety Provider	TEP Trusted Provider Certified Training Provider
Endorsing entity	eSafety Commissioner eSafety	Office of the eSafety Commissioner eSafety Commission 'Australian', 'Federal' or 'Commonwealth' Government Julie Inman Grant
Affiliation with eSafety	Endorsement, endorsed	Certified, accredited, approved Implying that you are a partner, employee, agent or contractor of eSafety

Program promotion and brand development

4. eSafety will seek to raise awareness and understanding of the Program in schools and with other potential audiences, including by:
 - publishing information about the Program and benefits of using a Trusted eSafety Provider on the eSafety website
 - maintaining a listing of endorsed Providers on the eSafety website including
 - filters to help users identify Providers that meet their needs based on location, delivery method, program audience and topics, and
 - contact information for each Provider
 - engagement with government and non-government school education authorities
 - including information about the Program in relevant eSafety resources and programs, and
 - eSafety social media channels.
5. eSafety will supply a promotional kit to each Trusted eSafety Provider to help them to raise awareness of the Program and promote their endorsement.
6. Providers are expected to promote their endorsement by, at a minimum:
 - displaying the logo on their organisation website (consistent with this Schedule 3)
 - referencing their endorsement within their Online Safety Education Program(s).
7. Providers are encouraged to promote their endorsement via other ways, for example:
 - in digital and printed brochures
 - on social media
 - in their email footer
 - in media articles (e.g., promoting their work with a client or visit to a regional area).
8. Providers should also be mindful that their professional conduct provides an opportunity to contribute to the Program being held in high esteem by schools and other potential audiences, while unprofessional conduct by any Provider has the potential to diminish confidence in the Program brand and other Providers.
9. As per clause 27 of this Agreement, Providers must use their best endeavours to ensure that, where they identify themselves as a provider of Online Safety Education Programs, content posted or shared online does not bring the reputation or standing of eSafety, the Program, or other Providers into disrepute. This may include, but is not limited to, content deemed to be offensive, inaccurate, inflammatory, disparaging of other Providers, or that otherwise has the potential to cause harm.

Use of the Trusted eSafety Provider logo

10. Providers are strongly encouraged to use the Trusted eSafety Provider logo to promote their endorsement and help build awareness of the Program.
11. This Agreement grants only permission for Providers to use the Trusted eSafety Provider logo. Providers must not use any other eSafety logo or branding without eSafety's express permission.
12. The Trusted eSafety Provider logo must be used in accordance with the specifications below.

Logo guidelines

Logo consistency is very important because it helps build a strong and uniformed brand identity.

The program logos do not include the Australian Government crest.

The Trusted eSafety Provider logo is in Navy and Aquamarine.

The inline version is to be used wherever space, size and layout permits. The White on eSafety Navy version can be used where a dark background is required.

Outlined on the following pages are the rules for how the logo is to be used.



Primary logo: Navy and Aquamarine, inline



Primary (reversed) logo: White and Aquamarine, inline



Secondary logo: stacked



Secondary reversed logo: stacked

Logo clearspace

The clearspace zone is indicated by the height of the 'S'.

The 'S' is from the word eSafety and should be used at the same size as within the logo.



Logo - inline



Logo - inline stacked

Logo minimum size

The minimum size shown here must be seen as a minimum but can be displayed at a larger size.

The same rules apply to every logo version for both print and digital.



Schedule 4 – Annual Reporting requirements

Purpose

1. Trusted eSafety Providers are required to complete an annual report for the financial year ending on 30 June for each year, or part year, covered by this Agreement (clause 33).
2. The annual report has two main functions:
 - to provide assurance of ongoing compliance with key requirements of this Agreement
 - to collect data about Online Safety Education Programs delivered by Providers.
3. eSafety requires this information to:
 - fulfil its legislative functions under the *Online Safety Act 2021* (Cth), for example, ‘to give the Minister reports about online safety for Australians’ under section 27(1)(j)); and
 - meet its public reporting obligations regarding the execution of its functions, including education program reach (e.g., in the eSafety Commissioner’s Annual Report, and to the Australian Parliament in evidence submitted through Senate Estimates processes and parliamentary inquiries).

Scope

4. A summary of information required in annual reports is outlined below. eSafety will confirm annual reporting requirements in greater detail at the beginning of each financial year or the commencement of this Agreement (whichever is earlier), to support the recording of relevant information during the reporting period.
5. Information to be provided in the annual report:
 - Online Safety Education Programs delivered to schools, including:
 - number of schools (by state/territory)
 - number of sessions (by state/territory, primary/secondary school)
 - number of participants (by students/teachers/parents).
 - Online Safety Education Programs delivered to organisations other than schools (e.g. community groups, sporting clubs, tertiary education institutions) including:
 - organisation types
 - number of sessions
 - number of participants.
 - Professional practice, including:
 - attendance at community of practice sessions (clause 31)
 - professional development/learning activities undertaken (clause 17.b)
 - feedback processes, review or evaluation undertaken (clause 21).
 - Safeguards and checks, including:
 - insurance cover – confirmation of policy continuity or provide updated details (clause 13)
 - child safety requirements – confirm continuing compliance and provide updated details (clause 14).

Schedule 5 – Process for handling complaints and breaches

The following process is based on the eSafety Complaint Handling Policy, as updated from time to time. The Policy applies to complaints about the administration of eSafety's functions, services, programs or resources, or about staff or other individuals or organisations that deliver programs, services or resources in collaboration with or on our behalf.

The eSafety Complaint Handling Policy is available on the eSafety website at <https://www.esafety.gov.au/about-us/corporate-documents>.

Scope

1. As set out in the eSafety Complaint Handling Policy, complaints can be made about the conduct of eSafety staff or other individuals or organisations that are affiliated with eSafety, including Trusted eSafety Providers.
2. Providers are bound to uphold the terms of this Agreement. eSafety also expects individuals and organisations that deliver programs, services or resources on behalf of or in collaboration with eSafety (including Trusted eSafety Providers) to demonstrate professional and ethical conduct.

Making a complaint to eSafety

3. If a complaint is made about a Trusted eSafety Provider (or another individual or organisation that delivers programs, service or resources on behalf of eSafety), we encourage the complainant to raise their concerns with the Provider directly. We expect the Provider to listen to these concerns and take reasonable action to resolve them.
4. If it is not appropriate to do so, or they are not satisfied with the response, a complainant can complain to eSafety. Depending on the issues raised, we may decide not to take further action on a complaint if the provider has not been provided with a reasonable opportunity to resolve it directly.

How we receive complaints

5. eSafety prefers that complaints are made in writing. For complaints that involve a Provider, the preferred point of contact is the Trusted eSafety Provider Feedback Portal located at <https://www.esafety.gov.au/educators/trusted-providers/feedback>.
6. Written complaints should tell us that the complainant wishes to make a complaint, explain what the complaint is about and list the parties involved. Complaints should also tell us the outcome being sought by the complainant.
7. eSafety is unable to receive complaints via our social media channels (including Twitter, Facebook, Instagram and LinkedIn).

Anonymous complaints

8. eSafety will investigate the issues raised by anonymous complaints and take appropriate action if we have enough information to do so. However, where we receive an anonymous complaint, our ability to satisfactorily resolve complaints may be limited in some instances, and we will not be able to respond to the complainant nor notify them of the outcome.

Part 1 – Investigation of complaints

Receiving and recording the complaint

9. Complaints will be recorded on our complaints management system. The type of information that will be captured at the start of and during the complaint handling process includes:
- when and how the complaint was made
 - personal details of the complainant (name and contact information)
 - what the complaint is about
 - the outcome sought
 - how the complaint was resolved, and
 - our actions, decisions and interactions with anyone involved in resolving the complaint.

Privacy and confidentiality

10. Complaints will be dealt with in a confidential manner that is respectful to all parties involved. Reasonable steps to protect personal information from loss, unauthorised access, use, disclosure or any other misuse during the complaint-handling process.² We will protect the identity of people making complaints where this is practical and appropriate. However, to resolve some types of complaints and comply with the principle of procedural fairness, it may be necessary for us to disclose a complainant's identity to the person who is the subject of the complaint.
11. Providers can learn about their rights in relation to personal information collected by the eSafety Commissioner by reading our [Privacy Policy](#). Our [Collection Notification](#) explains what information we collect, and what we do with it.

Acknowledging the complaint

12. Unless our staff can resolve a complaint 'on the spot', we will acknowledge receipt of complaints within 3 days. Information will be provided about the likely next steps in the complaint handling process, the expected timeframes for our actions and a contact point for enquiries.
13. Providers who are subject of a complaint will only be notified after an initial assessment has been completed, at the point at which it has been established that there is a relevant issue to be investigated.
14. During the complaint handling process, updates will be provided to all parties if our actions are delayed for some reason.

Assessing and allocating the complaint

15. We will assess the complaint issues raised, confirm that they are within our control to address, and identify the outcome sought. We will prioritise complaints according to the seriousness, complexity and urgency of the issues raised, having regard to:
- whether the complaint raises concerns about people's health and safety

² Examples of personal information include an individual's name, signature, address, telephone number, date of birth, school, medical records, financial details and commentary or opinion about a person.

- how the person making the complaint is being affected
 - the risks involved if resolution of the complaint is delayed, and
 - whether a resolution requires the involvement of other organisations.
16. Most people who make a complaint do so in good faith. However, on occasion, some people abuse the complaint-handling process. We carefully assess all complaints we receive. If we believe that a complaint has no or very limited merit, or that the primary purpose of the complaint appears to be to harass or annoy, we may decide not to take further action on the basis that it is frivolous or vexatious.
17. Once a complaint has been assessed, it will be allocated to a suitable staff member to resolve.

Resolving the complaint

18. Where possible, we will try to resolve complaints quickly and informally. Often, an apology, explanation or other remedial action can resolve straightforward complaints.
19. If this isn't possible or appropriate, the complaint will be allocated to a staff member who hasn't previously dealt with the matter. They will review all of the available information and decide the best way of resolving the complaint. To do this, they may need to seek further information from the complainant, another person within eSafety or another organisation.
20. As part of resolving the complaint, Providers will be presented with information about the complaint issues and given an opportunity to respond. We will consider any information provided by the individual or organisation when determining the outcome of the complaint.
21. A particularly serious or complex complaint may need to be formally investigated. This includes any complaint that raises serious issues about the conduct or integrity of an eSafety employee. A suitable person who does not have a conflict of interest will be appointed to conduct the investigation. The manner and extent of the investigation will be proportionate to the seriousness of the issue being investigated. All investigations will be guided by principles of confidentiality; procedural fairness; consistency; timeliness and support to those who need it.
22. The investigator will gather evidence and recommend findings based on the administrative standard of proof, i.e., the balance of probabilities. The recommended findings will be considered by the appropriate eSafety staff.
23. If a complaint requires further assessment, inquiries or investigation we will keep all parties informed about its progress.

Part 2 – Sustained complaints and remedies

24. If, after conducting this process, we plan to sustain the complaint, we will advise the individual or organisation and provide them with a further opportunity to comment on the outcome.
25. If the complaint issues are substantiated, we will address them by providing remedies that are reasonable, proportionate and well-targeted. Our focus is on accepting responsibility for errors or problems and taking action to correct them rather than

apportioning blame. The appropriate remedies will depend on the nature of the issues as well as the outcome being sought, but may include:

- an acknowledgement
- an explanation
- a verbal or written apology
- a different decision
- changes to improve policies or processes
- management action against an employee (e.g. providing/referring the subject of the complaint to counselling, professional training), or
- disciplinary action against an employee.

26. Sustained complaints that concern a Provider may also involve a breach of the Trusted eSafety Provider Agreement.

Part 3 – Process when there is a breach of this agreement

27. Where this is a minor breach, or the potential for corrective action to avoid future transgressions, we will work with the Provider to implement corrective strategies to remedy the breach and monitor compliance. This will involve eSafety communicating the corrective action in writing, and the Provider agreeing in writing to follow this course. After a period of time of between 3-6 months, depending on the seriousness of the issues and actions required, eSafety will make an assessment of whether the issues have been adequately resolved.

28. Where it has been established that an intentional or serious breach has occurred, the following remedies will be available to eSafety:

- Recording a 'strike' against a Provider. If another strike is registered in a period of 12 months, this may be grounds for termination of the Trusted eSafety Provider agreement.
- Where the breach presents an ongoing risk of personal or reputational harm, suspending a Provider until they are able to remedy the breach and demonstrate compliance.
- In the case of a serious breach where the non-compliance is incapable of remedy, immediately terminating the Trusted eSafety Provider Agreement consistent with Clause 9.

29. In the case of a serious breach and termination of Agreement, the organisation or individual must – as set out in Clause 12 – immediately cease advertising or promoting any affiliation with eSafety and take immediate steps to remove any use of the logo from all their websites, social media accounts and other communication channels.

Execution page

Executed as an Agreement between the eSafety Commissioner

Delegated Authority
eSafety Commissioner

___/___/___
Date

Name of Delegated Authority
(please print)

and [insert Organisation here]

Signature of Chief Executive/Authorised
Person

___/___/___
Date

Name of Chief Executive/Authorised Person
(please print)