Guide to engaging external online safety providers

Creating safer online environments

Why was this guide produced?

This resource provides guidance for school staff about engaging with external providers of online safety education.

Why engage an external provider for online safety education?

External providers are individuals, organisations and groups offering programs, resources, services and/or personnel with the aim of supporting schools to implement a whole-school approach to online safety education.

Online safety education is embedded across the Australian Curriculum in Health and Physical Education, Digital Technologies, and Media Arts, and it is addressed in the Foundation to Year 10 Curriculum's General Capabilities and Curriculum Connections documents (see, for example, the Online Safety Curriculum Connection).

External providers can complement and enhance school-based online safety education. However, they should not be the sole way that online safety education is delivered in schools. Effective online safety education is underpinned by a whole-school approach in which students learn online safety knowledge and skills, incrementally, at every year level and throughout the school year.

To make it easier for schools to select an external provider that meets their needs, eSafety has established the Trusted eSafety Provider Program. These providers have been endorsed by eSafety after demonstrating that they meet best-practice requirements for online safety education.

Before engaging with external providers, schools are encouraged to consult their school and/or education sector policies and procedures. For more information on best practice approaches to online safety education, see Best Practice Framework for Online Safety Education.

External providers of online safety education

Providers should:

- be knowledgeable on a range of online safety issues
- be aware of the functions and powers of the eSafety Commissioner
- demonstrate regard for the rights, safety and wellbeing of children and young people
- be professional, apolitical and transparent
- Be knowledgeable about:
    - The Australian Curriculum and/or relevant state/territory syllabus documents
    - eSafety's Best Practice Framework for Online Safety Education
    - The Australian Student Wellbeing Framework
    - The National Principles for Child Safe Organisations and state and territory child safe standards

Selecting an external provider

The following checklist offers some considerations and key questions to use when selecting an external provider. Schools may also consider using Educate – STEPS framework for selecting online safety programs, which has been adapted to for online safety education with permission from Bullying, No Way! It provides a framework for more deeply examining program content and approaches.

Checklist for selecting external providers	Yes
Program content	
Does the program and its key messages reflect the school's philosophy and values? • Ask to preview a detailed outline of the content and key messages, in advance, or meet with the provider beforehand to choose the most appropriate content to meet your school's needs. • Inform the presenter if there have been any recent online safety incidents at your school that require sensitivity. The presenter should tailor their content appropriately. Online safety scenarios may be used (with consideration, care, and de-identification).	☐
Is the program content appropriate for your school? • Ask how the content aligns with the Australian Curriculum or state and territory syllabus, and how they tailor content for different audiences and year levels. • Ask about the teaching strategies they use, if they link to any well-being initiatives and how they reference eSafety's resources and reporting schemes.	☐

Have parents and carers at your school been consulted or informed about the program and given consent for their child to participate? • Ask how parents and carers can be engaged to support program delivery, and to preview any materials that will be shared with them. • Will parents/carers and staff sessions be offered as part of the program. Would these groups benefit from combined or separate sessions? Is this option provided by the provider, or could it be provided by the school? • See Educate – Tips for parent-carer education and engagement.	☐
Is the program accessible to students with specific needs and vulnerabilities? • Ask if the provider has experience working with students with specific needs and vulnerabilities, and how they tailor their content to suit different audiences. • Ask how diversity and inclusion is reflected in the language, images, and formats used in the program.	☐
Is the program based on relevant, recent research and an understanding of current technologies? • Ask about the research and other evidence that has informed the program. • Ask if the provider uses examples of apps, platforms, and services that are popular, current, and relevant to students. emerge, become quickly adopted, change and sometimes disappear — providers need to keep their content up to date.	☐
Does the program use shock, fear, or scare tactics or focus on specific critical incidents to produce emotive responses? • The most effective programs encourage a strengths-based, positive approach to online safety education, with a focus on building help-seeking behaviours and resilience. • There is little evidence to suggest that shock tactics and fear arousal are effective with young people. It's important for schools to ensure providers do not encourage students to provide personal stories, and that they have processes in place to manage disclosures when these do occur.	☐
What follow up session/s are scheduled for students? • Ask school staff how the external provider's work will be supported in follow up lessons in classes, and how it can be integrated with other curriculum delivery, including the General Capabilities. When will this be done and by whom?	☐
Has the program been evaluated? • Ask how the impact of the program will be measured? Will students complete an evaluation on the program and/or will attitudes or learning outcomes be measured by school staff/the provider? • Regular program and content reviews that consider current trends, apps, games and platforms are important for a dynamic topic like online safety. Program evaluation shows a commitment to improvement. If the program has not been evaluated, ask whether the provider is open to feedback.	☐

Is the provider's fee reasonable and appropriate, and how is this assessed? • Providers should be transparent about their fees and able to justify the cost of services. Comparing quotes and researching the market may help you determine what's reasonable. Your school and/or education sector may have guidance to help with your decision.	☐
Does the provider's content promote third-party products or businesses that will charge users a fee? • Providers should be transparent about any commercial arrangements they have with product, app or service providers. For example, if there is an arrangement to endorse or recommend a product, or where financial or in-kind support has been provided, the terms should be clearly disclosed to the audience. • Advertisements, offers or calls to action for a company's products or services should be clearly disclosed.	☐

Business registration

Does the provider have an ABN (Australian Business Number) and ACN (Australian Company Number) if applicable? • Ask for the ABN and ACN. Ideally, this should be included automatically in correspondence with schools, for example in email templates or signature blocks. This allows the business to be identifiable, including for the purposes of invoicing (if applicable).	☐

Insurances

Does the provider have requisite insurances, for example, workers compensation, public liability and professional indemnity insurances? • Workers compensation insurance is compulsory for most employers in Australia, though requirements vary across jurisdictions. Where applicable, Trusted eSafety Providers have demonstrated this as part of the endorsement process. • All states and territories require that external providers have public liability insurance that is current and with a reputable insurer for a minimum sum (which varies across jurisdictions). Check if the provider has this insurance. Trusted eSafety Providers have demonstrated that they hold appropriate public liability insurance policy. • Professional indemnity insurance provides financial protection against legal liabilities arising because of negligent acts, errors or omissions committed while providing consultancy services. Check if the provider has this insurance. Trusted eSafety Providers have demonstrated that they hold appropriate professional indemnity insurance.	☐

Child safety

Has the provider obtained necessary child protection and safeguarding checks to work with children and young people?

- Ask to verify the provider's Working with Children Check (or state/territory equivalent) and record the details – even if they are delivering a presentation online.
- Ask for evidence of completion of mandatory child protection training.
- Ask what policies and procedures they have in place for assessing and mitigating risks to students' safety and wellbeing. For example, is appropriate support in place to appropriately respond to student disclosures of harm?
- Ask how school staff and students' personal information (e.g. email addresses, names on attendance lists) will be handled by the provider and how and where information will be stored?
- Consult school and/or education sector policies for information about which specific additional policies they are required to know. For example, duty of care, code of conduct, acceptable use of technology, data privacy and protection, and other legal reporting requirements.

Reminder: external providers should not be present without a staff member in the classroom.

☐

Capability

Has the provider demonstrated their capability to deliver online safety programs in Australian schools?

- Ask for information about the provider's qualifications, background and experience:
  - how long they have been providing programs
  - the number, and type, of institutions where they have previously delivered programs.
  - referee reports and testimonials from other schools may also be useful.
- Ask about the presenters' specific training and/or preparation for school-based delivery.

Can the provider explain how their content is aligned to the Australian Curriculum or state/territory syllabus?

☐

Trusted eSafety Providers

eSafety's Trusted eSafety Provider program is designed to provide schools with confidence that the external online safety provider they engage meets specific quality criteria.

Trusted eSafety Providers are endorsed by eSafety and meet a high threshold in terms of their knowledge, capability and experience in delivering quality online safety education. They are also required to comply with relevant safeguards.

These providers are part of a collaborative community of practice sharing the latest research and best practice approaches to online safety education.

See our Trusted eSafety Providers.

Providing feedback, concerns or complaints about a provider?

Giving and receiving feedback is important for continuous improvement of programs and resources. External providers may seek feedback from you and from student participants on the quality or impact of their program in the form of short surveys. Taking a few minutes to provide your comments or ratings will contribute to the evidence base that a provider can use to evaluate and improve their program.

However, if you have concerns or complaints about:

- an external provider, this should be directed to the specific provider in the first instance and, if appropriate, shared with the school leadership team and/or relevant education sector personnel.
- a Trusted eSafety Provider, this should be directed to the eSafety Commissioner at trustedproviders@esafety.gov.au

Updated 03/2026