Guide to engaging external online safety providers

eSafety Toolkit for Schools

Creating safer online environments

This resource provides guidance about how schools can engage external providers. Providers can support online safety education through presentations, workshops and information sessions.

Why engage an external provider?

Before engaging an external provider, schools are encouraged to access relevant eSafety resources and to seek support from their education sector. Providers should complement and enhance the curriculum-based online safety education delivered by school staff. They can bring unique perspectives and may support schools where there are concerns about specific risks, or when staff need help to address certain issues.

However, best practice emphasises that there is a need for scaffolded and consistent education over a student's years of schooling. One-off approaches are not enough to develop students' knowledge, awareness and skills. For more information on best practice approaches to online safety education, see eSafety's Best Practice Framework for Online Safety Education.

Considerations for engaging external providers

To help assess whether engaging an external provider will help support online safety education at your school, consider the following:

- What is the purpose of the program? Is it addressing a specific issue? What practical strategies are students and staff expected to learn?
- Can the provider explain how their content is aligned to the Australian Curriculum or state/territory curriculum?
- Does the provider adapt the program for different year levels, contexts and audiences?
- Can you preview the program or a detailed outline of the content and key messages?
- Have parents/carers been informed about the program and given consent for their child to participate?
- How will confidentiality, privacy, disclosure of personal information and data collection be handled by the provider?
- Are appropriate processes and support services in place for managing student disclosures?
- Would staff or parents/carers benefit from separate sessions? Is this option provided by the provider, or could it be provided by the school?
- How will the impact of the program be measured? Will students complete an evaluation on the program and/or will attitudes or learning outcomes be measured by staff/the provider?
- How will program outcomes be used to inform future online safety education?
- What follow up session/s are scheduled for students? When will this be done and by whom?

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 certain 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.

A list of Trusted eSafety Providers is available at: esafety.gov.au/educators/trusted-providers.

What should I expect from an external provider of online safety education?

Providers should:

- be professional, apolitical and transparent
- be knowledgeable on a range of online safety issues, familiar with the functions and powers of the eSafety Commissioner and committed to upholding child safety policies and legislation
- have processes in place if a student makes a disclosure or becomes distressed — and should discuss these with staff before presenting to students
- demonstrate regard for the rights, safety and wellbeing of children and young people.

Providers should also be knowledgeable about the:

- Australian Curriculum and state/territory curriculum requirements
- eSafety's Best Practice Framework for Online Safety Education
- Australian Student Wellbeing Framework
- National Principles for Child Safe Organisations and state and territory requirements
- policies and procedures in place for balancing students' expectations and rights to privacy and confidentiality with the school's duty of care and mandatory reporting requirements.

What should I do if I have feedback about a provider?

Feedback, complaints or concerns about:

- a **Trusted eSafety Provider** should be directed to the eSafety Commissioner at trustedproviders@esafety.gov.au
- other external providers should be directed to the provider and, if appropriate, the education department or sector.

How do I select an external provider?

At times, you may need assistance to choose the right provider. For example, when an external organisation approaches your school but is not endorsed as a Trusted eSafety Provider, or where there are multiple providers to choose between.

The following checklist offers some questions to ask potential providers. Schools may also consider using Educate 8 - STEPS decision making framework, which has been adapted to an online context with permission from Bullying, No Way!

Checklist for selecting external providers	Yes
Has the provider obtained necessary safeguarding checks to work with young people? • Ask for evidence of the provider's Working with Children Check (or state/territory equivalent) — even if they are delivering a presentation online. Ask what policies and procedures they have in place for assessing and mitigating risks to students' privacy and wellbeing, and for meeting child safety requirements such as mandatory reporting, duty of disclosure, data privacy and protection or other legal reporting requirements. **Reminder:** external providers cannot present without a staff member in the classroom.	☐

Has the provider demonstrated their capability to deliver online safety programs in Australian schools?
• Ask for information about the provider's background and experience:
  • how long they have been providing programs
  • the number, and type, of institutions where they have delivered programs.
• Information about the experience and background of presenters, referees or testimonials from other schools may also be useful.
	☐

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. Another option is to meet with the provider beforehand.	☐
Is the program content appropriate for your school? • Ask how the content aligns to the Australian Curriculum or state and territory syllabus, and how they tailor content for different audiences and year levels. • Ask which teaching strategies they use, if they link to any wellbeing initiatives and how they reference eSafety's services and complaint pathways. • 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 accessible to students with specific needs or vulnerabilities? • Ask if the provider has experience working with students with vulnerabilities or specific needs and how they tailor their content to suit different audiences. • Ask how diversity and inclusion is reflected in the language and images used in the program.	☐
Is the program based on relevant, recent research and an understanding of current technologies? • Ask what research has informed the program. • Ask if the provider uses examples of apps/platforms that are popular, current and relevant to students. Apps/platforms emerge, change and sometimes disappear — providers need to keep their content up to date.	☐

Checklist for selecting external providers	Yes
Does the program use shock/scare tactics or focus on specific incidents to cause 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 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 they do occur.	
Has the program been evaluated? • Regular program and content reviews that consider current trends, apps, games or platforms are important for a dynamic topic like online safety. Program evaluation also 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 or appropriate, and how is this assessed? • Providers should be transparent about their fees and able to justify the cost for services. Comparing quotes and researching the market may help you determine what's reasonable. Your education department or sector may have guidance to help with your decision.	
Does the provider have sufficient workers compensation insurance, public liability or professional indemnity insurance? • Workers compensation insurance is compulsory for most employers in Australia, though requirements vary between jurisdictions. Where applicable, Trusted eSafety Providers will have this. • 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. Where applicable, Trusted eSafety Providers will have this. • Professional indemnity insurance provides financial protection against any legal liabilities arising because of negligent acts, errors or omissions committed while providing consultancy services. Check if the provider has this insurance. Where applicable, Trusted eSafety Providers will have this.	
Is the provider's content non-commercial, or does it promote third-party products or businesses? • In situations where a commercial entity has provided financial or in-kind support for a program, the terms of this support should be clearly disclosed. • Advertisements, offers or calls to action for a company's products or services should be stated.	

Updated 09/2022