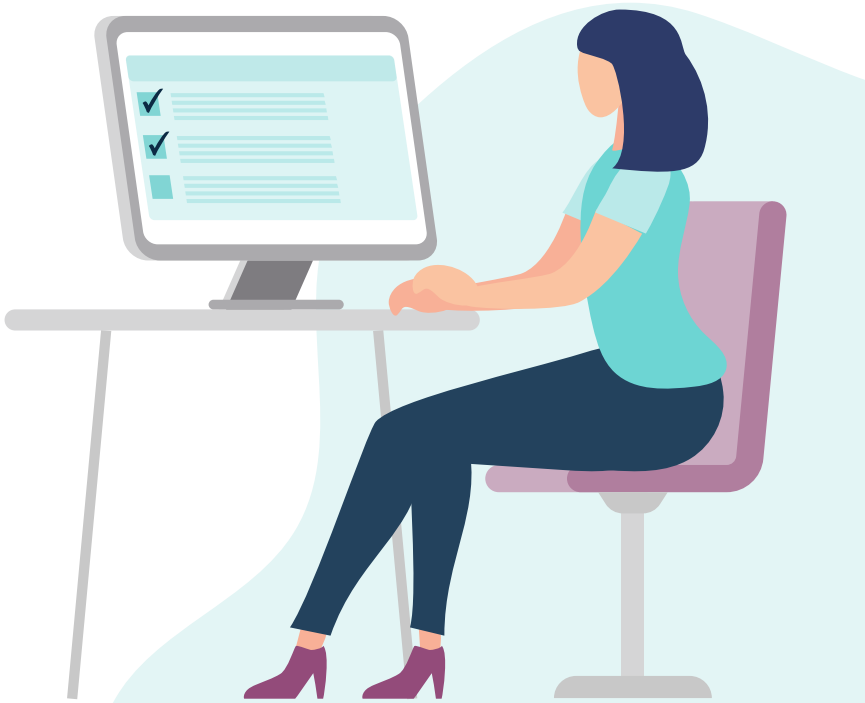
Online safety self-assessment tool

eSafety Toolkit for Schools

Creating safer online environments



This self-assessment tool is designed for school leadership teams to assess their school's online safety environment. It provides tailored suggestions to help schools improve their practices.

Some assessment questions refer to school policies, but these may be education department or sector policies. It should therefore be read in conjunction with applicable national, state and territory laws, policies and procedures.

Question	Room to improve	Yes	Suggestions to improve practice	Review date
Is school leadership committed to creating and maintaining a safe online environment?			• Encourage a positive school climate and a culture of help-seeking that supports students to feel safe and comfortable to report online incidents. • Have a strong 'no bullying' attitude and role modelling respectful behaviours. • Include safety in the mission and values of the school. • Promote online safety at assemblies and in newsletters — informing the whole school community about where to find support and advice.	
Is the school actively implementing the National Principles for Child Safe Organisations?			• Read and adopt relevant standards from the National Principles for Child Safe Organisations. While the standards may not be mandatory in all jurisdictions, they have been endorsed by members of the Council of Australian Governments (COAG) and reflect leadership and commitment to child safety and wellbeing. • Use the Australian Government's practical tools and resources to help implement the principles in your school. • Implement local or state-based child safe requirements.	
Does the school have staff members with responsibility for online safety?			• While all members of a school community should promote online safety, schools are encouraged to have specific roles with this responsibility. • Establish an online safety team that has responsibility for, and champions, online safety. This might include health and physical education or digital technologies staff, student wellbeing coordinators, as well as students and parents/carers.	
Does the school have policies and procedures in place to safeguard against, and respond to, online safety incidents?			• Create policies and procedures to safeguard against, and respond to, online safety incidents. All schools should have these. • Prepare 2 - Checklist for developing effective online safety policies and procedures can help schools prepare these and support good practice.	

Question	Room to improve	Yes	Suggestions to improve practice	Review date
Do policies and procedures outline expected behaviours and roles of school community members when engaging online or using digital technologies?			• Set out the school's expectations and make clear what behaviour is/is not acceptable for students, staff and families when engaging with the school community online or using digital technologies. • eSafety's Prepare 2 - Checklist for developing effective online safety policies and procedures and Engage 5 - School charter of commitment to online safety can help schools prepare policies and procedures and support good practice.	
Does the school effectively plan and assess the risks and benefits before introducing new online platforms or technologies?			• Endeavour to use software, online products and collaboration tools with the highest safety, privacy and security standards possible. • Conduct risk assessments to promote safety, privacy, security and age-appropriateness prior to using any platform or technology within the school, for school purposes or in a way that impacts the school community. • eSafety's Prepare 3 - New technologies risk-assessment tool can help to assess risks and benefits before introducing new digital technologies or social media platforms.	
Does the school minimise the risks of exposure to sensitive/ harmful information through actively monitoring and filtering harmful content?			• Use appropriate technologies to monitor and filter harmful content. Often this filtering technology and infrastructure is provided by the education department or sector. • It's important to have a thorough understanding of how the filtering technology and infrastructure works. The infrastructure should allow access to age-appropriate content for educational purposes. • Filtering can help monitor and limit what students access online, however no filter is 100 per cent effective. Filters or other controls should not be solely relied on or used to replace online safety education. • A good practice is for the ICT Manager to provide a regular report with usage trends to the school leadership team. • Establish response processes that focus on safety and wellbeing when responding to instances where student/s repeatedly try to access harmful content.	

Question	Room to improve	Yes	Suggestions to improve practice	Review date
Has the school considered how to minimise the risk of students being inappropriately contacted by via email?			• Be aware of the safety and security risks posed by using simple email naming conventions (for example, students' real names), which can make it easier for strangers to identify and contact students. It's also important to have appropriate technologies in place to monitor and filter email activities on school ICT systems. • While often school email addresses are set by the education department or sector and are designed to be simple to help younger students, schools are encouraged to consider alternative options that may be safer. For example, email addresses using a student number, a difficult to guess combination of partial name elements — or a blend of both. • Communicate to staff, parents/carers and students the risk of inappropriate contact using school email addresses. • Teaching students strategies to report unauthorised communication and block unknown email addresses will also help to minimise risk.	
Do policies or procedures set out who will moderate the school's social media and websites, and when they will be moderated?			• At least two members of staff should have access to school social media and websites, including a member of the school leadership team. These accounts should be monitored regularly. • eSafety's Prepare 4 - Guidelines for social media use - video sharing and online collaboration and education department or sector policies can help to support good practice.	
Are there clear guidelines about the acceptable use of the school's name, logo and brand?			• Communicate to all members of the school community the acceptable use of the school's name, logo and brand. • eSafety's Prepare 4 - Guidelines for social media use - video sharing and online collaboration and education department or sector policies can help to support good practice.	

Question	Room to improve	Yes	Suggestions to improve practice	Review date
Does the school provide information to students and their parents/ carers about how their personal information (such as names, photos, work samples or other identifying information) will be used online?			• Always seek consent from students and their parent/carers, and staff consent, prior to publishing their information online. This could be through an annual blanket consent form for regular communications such as newsletters, with additional consent sought for one-off events or additional communications. • Provide information on the possible use of the image/s to enable students and parents/carers to have a clear understanding of what they are consenting to, and who has access to the images or information. • Communicate with parents/carers when online accounts are created for students (e.g. for resource subscriptions and apps) and to share the strategies being used to keep students' identities safe. • Where possible, use only first names when publishing student information online. • Consider circumstances that could place a student at risk of harm if their image or information is shared. For example, where there are legal proceedings or a court order relating to child protection, custody, domestic violence or family separation.	
Does the school have clear policies and procedures about how photos and videos of students will be managed, stored and shared?			• Store photos and videos of students securely with limited or password protected access. • Make sure procedures are clear, easy to follow and that all staff, students and parents/carers are aware of where to find them and how to use them. • eSafety's Prepare 4 - Guidelines for social media use - video sharing and online collaboration and education department or sector policies can help to support good practice.	

Question	Room to improve	Yes	Suggestions to improve practice	Review date
Does the school have procedures in place for responding to online safety incidents, for example serious cyberbullying or explicit image sharing?			• Have clear procedures in place so that if an online safety incident is reported, students and staff know what to do and where to access help. • Use eSafety's Respond resources to support good practice.	
Does the school engage the whole school community to create and maintain a safe online environment?			• It is good practice to involve the whole school community in online safety including opportunities for meaningful student participation and parent/carer engagement. • Use eSafety's Engage resources — these provide advice on involving the whole school community in online safety.	
Does the school take a comprehensive approach to online safety education through curriculum and teacher professional learning?			• Supporting staff and educating students to have positive and safe online experiences is an important part of a comprehensive approach to online safety. • Use eSafety's Educate resources — these provide advice on building the online safety knowledge, skills and capabilities of the school community.	
Does the school use preventative, harm minimisation and incident management strategies to support everyone involved in online incidents?			• Schools can better respond to incidents by focussing on wellbeing, restoring relationships and having partnerships with external support services, including local police. • Use eSafety's Respond resources — these provide advice on supporting the school community after an online safety incident, including how to undertake a post-incident review.	

Updated 09/2022