New technologies
risk-assessment tool

eSafety Toolkit for Schools
Creating safer online environments

This risk-assessment tool can help schools to effectively plan and assess risks and benefits before introducing any new online platforms or technologies. Additional research about the platform/technology is recommended if you are unsure of the answer to one or more of the questions.

For technical questions, ask for guidance from an appropriately qualified advisor, member association or technology support staff. You might also check with staff who have already adopted the technology. Once your school has decided on the technology or platform it wishes to use, staff will need to be shown how to use the technology, and how to integrate its use into the curriculum. Staged implementation may help to avoid unintended or unexpected consequences of student use. Usage should be consistent with, and informed by, education department or sector policies and procedures.

Risk identified: take appropriate action to mitigate risks before using

Proceed with caution: continue to monitor for risks

Consider	Yes	No	Suggestions to mitigate risks
Will students' personal information be publicly displayed (e.g. photograph, date of birth, gender or name of school)?			• Obtain consent from students and their parents/carers before displaying personal information online. • Where possible, de-identify student information.
Can external, unauthorised users communicate with students?			• Install appropriate technologies to monitor and filter activities on school ICT systems. • Teach students strategies to report external, unauthorised communication and block inappropriate content or contact.
Does the platform encourage students to use their existing email or social networking accounts for sign in or use?			• Often platforms also have the option to sign up or log in using unique usernames and passwords. While using existing social networking accounts might be quicker, unique logins are a safer option. • Teach students the importance of strong passwords and not sharing passwords.
Are student profiles linked to apps that can display their location?			• Teach students strategies to turn off location services functions, or to block apps that have these turned on.
Does the education department prohibit the use of this technology or platform?			• If the education department's policies prohibit the use of this technology or platform it is recommended not to use it.
Can students access inappropriate content using this technology or platform?			• Install appropriate technologies to monitor and filter activities on school ICT systems. • Encourage help-seeking behaviours so students know the steps to take if they come across inappropriate content.
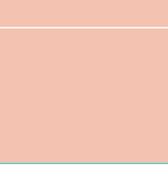
Consider	Yes	No	Suggestions to mitigate risks
Have minimum age requirements for the technology or platform been adhered to?			• Check age appropriateness prior to use. • Teach students about age recommendations and the reasons behind them.
Does the platform promote privacy and security for students and their accounts?			• Empower students to protect their privacy and explain how to adjust security settings.
Have parents/carers consented to their child using this technology or platform?			• Ensure appropriate consent has been provided by parents/carers. Some schools request consent to use a broad range of platforms at the start of the school year to avoid having to ask for consent each time a new platform is used. It's important to be as clear as possible about what this consent includes, as well as providing information on any possible risks to users and how the school mitigates them.
Are staff comfortable and confident using the platform?			• Provide access to professional learning so staff are skilled in the platforms/technologies they use.
Is there a staff member moderator for chat or comment functions?			• A staff member (or team) would ideally be appointed to moderate chat or comment functions, to encourage safe and positive interactions and to take down and investigate inappropriate posts.
Does the platform have capacity to report problems or misuse?			• All platforms should have terms of use that clearly identify inappropriate content or behaviour, and how to report problems or misuse. • Visit The eSafety Guide for more information.
Do all users know how to set the platforms' privacy settings?			• Share The eSafety Guide with staff. This has links to the latest games, apps and social media, with tips on how to set privacy settings.
Have you identified how data is stored and used by the platform?			• Privacy issues arise when data is collected and not stored securely or shared inappropriately. Good practice is to find out how data will be stored and who has access. • Check education department or sector policies to see if there are any standard protocols schools should follow, as well as advice about privacy legislation and data storage.

eSafety education

esafety.gov.au