New technologies risk-assessment tool

Creating safer online environments

Disclaimer: This material is general in nature. It is made available on the understanding that the Commonwealth is not engaged in rendering professional advice. Before relying on the material in any matter, you should carefully evaluate its accuracy, currency, completeness and relevance for your purposes and should obtain any appropriate professional advice relevant to your particular circumstances. The Commonwealth does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency or completeness of any material contained in this resource or on any linked site. References to other organisations or websites are inserted for convenience and do not constitute endorsement.

Australian Government

eSafety Commissioner

eSafety.gov.au

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, education sector or technology support staff. You might also check with staff who have already adopted the technology. Once your school/education sector 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. Staged implementation may help to avoid unintended or unexpected consequences of student use. Usage should be consistent with, and informed by, school and/or education sector policies and procedures.

Important note

This risk-assessment tool is not exhaustive and should be adapted to school contexts and circumstances. It cannot replace legal advice regarding statutory and common law obligations to assess risks. The decision to use certain technologies or platforms should be made in line with school and/or education sector policies and guidelines. School leadership teams may wish to take legal advice when making these decisions.

🟧 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
Does personal information need to be provided to enable access to the technology or platform?	□	□	• Note that personal information includes: student name, date of birth, phone number, school name, location, student ID, IP address, images and biometrics. • Ensure that only approved apps, services and platforms are used. • Look closely at product user agreements, terms and conditions and disclaimers. Pay special attention to how user data will be protected. • Obtain consent from students and their parents/carers before using or sharing personal information to set up new technologies and online platforms. See Prepare 2 – Checklist for developing effective online safety policies and procedures. • Recognise that parents/carers may have different levels of awareness and comfort with the number and types of learning apps used in schools. • Find basic online safety tips for all users here: How to manage your digital safety settings.
Can external, unauthorised users contact or communicate with students?	□	□	• Install appropriate technologies to monitor and filter activities on sector/school ICT systems. • Be alert for unauthorised access or attempts to bypass controls. • Teach students the importance of strong passphrases and not sharing these with anyone. • Teach students how to block and report external, unauthorised communication and inappropriate content or contact.
Are student profiles linked to apps that can display their location?	□	□	• Many apps collect geolocation data to provide personalised features. Schools should manage permissions for this data collection. • Teach students strategies to turn off location services functions and to identify and block apps that have these turned on. • For further information, see Location sharing.

Is the technology or platform approved for use?	□	□	• Use only approved technologies, apps, platforms and services that have been approved by the education sector or school leadership and avoid any that are unapproved or have been explicitly prohibited.
Can students access inappropriate content using this technology or platform?	□	□	• Install appropriate technologies to monitor and filter activities on school ICT systems. • Encourage and normalise help-seeking so students know the steps to take when they come across inappropriate content or encounter situations online that concern them.
Have minimum age requirements for the technology or platform been adhered to?	□	□	• Check age requirements prior to use. • Even when age requirements are met, school staff should review technologies and platforms for age-appropriateness and their application to the local context. • Teach students about age recommendations, age restrictions and the reasons behind these. • Refer to the eSafety hub to stay up to date with the latest information on the social media age restrictions.
Does the platform promote privacy and security for students and their accounts?	□	□	• Ensure that school staff are able to make full use of security settings and do so consistently. • Empower students to protect their privacy and guide them in how to adjust security.
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 introduced. It's important to be as clear as possible about what consent includes, as well as providing information on any possible risks to users and how the school mitigates them.
Are staff confident using the technology or platform?	□	□	• Provide access to ongoing professional learning so staff are skilled in the technologies and platforms they use.

Are there staff members appointed to monitor and moderate chat and comment functions?	□	□	- Appoint least two members of staff and a member of the school leadership team to monitor and moderate chat and comment functions, to encourage safe and positive interactions and to take down and investigate inappropriate posts.
Does the platform have capacity for users 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 on how to report harmful content.
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.
How is data stored and used by the platform?	□	□	- Privacy issues arise when data is collected but not stored securely according to Australian data protection and privacy laws. - Avoid data sharing with third parties. - It is good practice to find out how and where data will be stored and who has access. - Check legislation, policies and procedures relevant to your school and/or education sector.