



Risk assessment for new technologies and online platforms




This checklist can help you plan and assess the safety risks and benefits of any new online platforms or technologies before they are introduced. Additional research about the platform or technology is recommended if you are unsure how to respond to questions in the checklist.

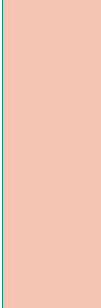
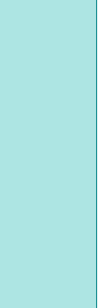
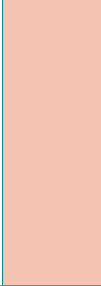
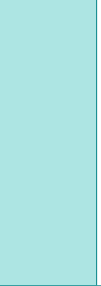
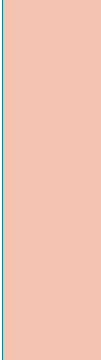
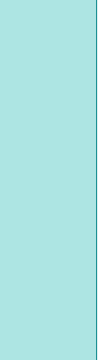
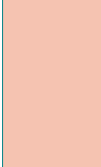
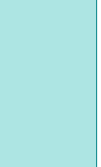
For technical questions, please seek guidance from an appropriately qualified advisor or your institution's Information Technology (IT) division. Once your institution chooses a technology or platform, staff will need training on its use, including how to safely integrate it into course delivery. Staged implementation may help to avoid unintended or unexpected consequences of student use.

Important note

This checklist is a guide and is not exhaustive and should be adapted to your institution's circumstances. It does not replace legal advice regarding any obligations to assess risks. The decision to use certain technologies or platforms should be made in line with your institution's risk management and IT acquisition procedures.

 **Risk identified:** take appropriate action to mitigate risks before using

 **Proceed with caution** and continue to monitor for risks

Consider	Yes	No	Suggestions to mitigate risks
Will personal information be publicly displayed? For example, student or staff photographs, date of birth, gender or name of institution.			<ul style="list-style-type: none">• Obtain consent from users before displaying personal information online.• Where possible, de-identify information.
Can external, unauthorised users communicate with students?			<ul style="list-style-type: none">• Install appropriate technologies to monitor and filter activities on Information Technology (IT) systems.• Teach staff and students how to report external, unauthorised communication and block inappropriate content or contact.
Does the platform encourage students or staff to use their existing email or social networking accounts to sign in or use?			<ul style="list-style-type: none">• Often platforms also have an option to sign up or log in using unique usernames and passphrases. Aim for users to have unique logins. Using existing social networking accounts to login might be quicker, but not as safe.• Emphasise to users the importance of having complex passwords or passphrases and not sharing them.
Are user profiles linked to apps that can display their location?			<ul style="list-style-type: none">• Teach users how to turn off location services and settings, or to block apps that have these turned on.

Can students or staff access inappropriate content using this technology or platform?			<ul style="list-style-type: none"> • Install appropriate technologies to monitor and filter activities on IT systems. • Encourage help-seeking behaviours so staff and students know what steps to take if they come across inappropriate content.
Does the platform promote privacy and security? Do students and staff know how to manage their settings?			<ul style="list-style-type: none"> • Empower users to protect their privacy and security by explaining how to adjust their settings or, where possible, providing links to instructions from the software developer. • Share The eSafety Guide with staff. This has links to commonly used social media, games, apps and sites, with tips on how to set privacy settings.
Are staff comfortable and confident using the platform?			<ul style="list-style-type: none"> • Provide access to professional learning so staff are skilled in the platforms and technologies they use.
Does the platform have capacity to report problems or misuse?			<ul style="list-style-type: none"> • Point out the platform's own terms of use and any information it provides about inappropriate content or behaviour and how to report problems or misuse. • Refer users to The eSafety Guide to learn more about the reporting options on commonly used social media, games, apps and sites.
Does the platform allow staff to moderate chat and comment functions? Are staff aware of how to use these functions?			<ul style="list-style-type: none"> • Make sure staff understand how to moderate chat or comment functions, to encourage safe and positive interactions and to take down and investigate inappropriate posts. • Have moderators available for large online events and classes, to support online safety.
Have you identified how data is stored and used by the platform?			<ul style="list-style-type: none"> • Privacy issues arise when data is collected and is shared inappropriately or not stored securely. Good practice is to find out how data on each platform will be stored, for how long and who has access, and to communicate this information to the users.