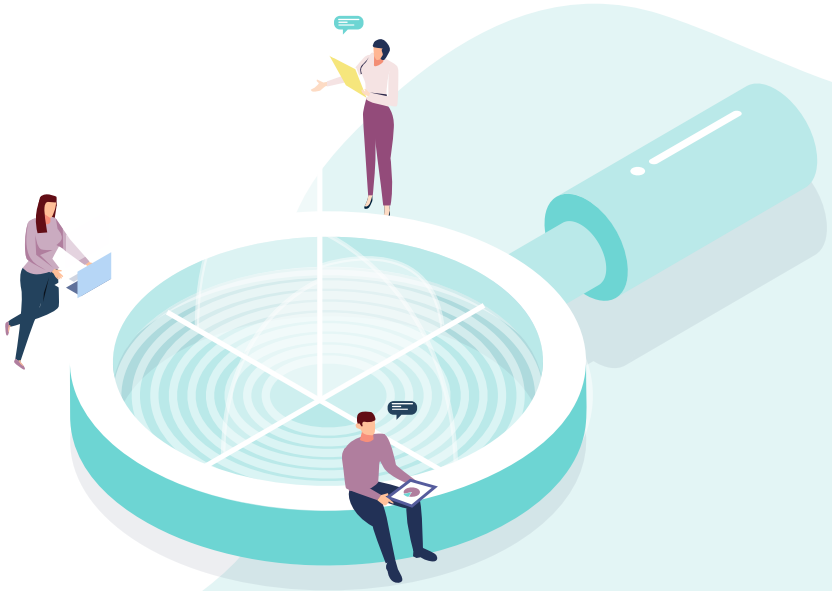
Risk assessment
for new technologies and online platforms

Toolkit for Universities

Creating safer online environments



This checklist can help universities to effectively plan and assess safety risks and benefits before introducing any new online platforms or technologies for staff/student use. Additional research about the platform/technology is recommended if you are unsure of how to answer one or more of the questions.

For technical questions, seek guidance from an appropriately qualified advisor or your institution's IT division. Staff who have already adopted the technology may also be able to help. Once your university has chosen a technology or platform, staff will need training on its use, including how to integrate it into course delivery. Staged implementation may help to avoid unintended or unexpected consequences of student use.

Important note

This checklist is not exhaustive and should be adapted to individual university circumstances. It does not replace legal advice regarding any legal obligations to assess risks. The decision to use certain technologies or platforms should be made in line with a university's risk management/IT acquisition 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 personal information be publicly displayed — i.e. student or staff photographs, date of birth, gender or name of university?			• Obtain consent from users before displaying personal information online. • Where possible, de-identify information.
Can external, unauthorised users communicate with students?			• Install appropriate technologies to monitor and filter activities on university ICT systems. • Teach staff and students how to report external, unauthorised communication and block inappropriate content or contact.
Does the platform encourage students/staff to use their existing email or social networking accounts to sign in/use?			• Often platforms also have an option to sign up or log in using unique usernames and passwords. While using existing social networking accounts might be quicker, unique logins are safer. • Emphasise to users the importance of strong passwords and not sharing passwords.
Are user profiles linked to apps that can display their location?			• Teach users how to turn off location services, or to block apps that have these turned on.
Can students/staff access inappropriate content using this technology or platform?			• Install appropriate technologies to monitor and filter activities on university ICT systems. • Encourage help-seeking behaviours so staff and students know what steps to take if they come across inappropriate content.

Consider	Yes	No	Suggestions to mitigate risks
Does the platform promote privacy and security? Do students/ staff know how to manage their settings?			• Empower users to protect their privacy and explain how to adjust security settings. Provide users with instructions about how to set privacy and security settings, or links to instructions from the software developer where possible. • Share the eSafety Guide with staff. This has links to the latest platforms, apps and social media, with tips on how to set privacy settings.
Are staff comfortable and confident using the platform?			• Provide access to professional learning so staff are skilled in the platforms/technologies they use.
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.
Does the platform allow staff to moderate chat and comment functions? Are staff aware of how to use these functions?			• Staff should understand how to moderate chat or comment functions, to encourage safe and positive interactions and to take down and investigate inappropriate posts. • Having moderators available for large online events and classes will support users' online safety.
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 on each platform will be stored and who has access.

Published 05/2020