Safe use of online collaboration tools for teaching staff

This resource provides guidance on how to address online safety issues within your institution's collaboration tools and learning management systems (LMS). It aims to prevent issues such as mistakenly sharing personal information or leaving system settings on which enable anyone to access online classes, tutorials, online spaces or lectures, as well as minimising the risk of inappropriate comments being made on discussion forums.

With increased use of online learning and collaboration platforms for both classes and group work, it is important to be aware of online safety issues, understand how to address inappropriate online behaviour and know where to find support for using and managing online platforms.

This resource should be read and used in conjunction with the institution's policies, codes of conduct and other relevant documents which outline staff and student expectations and protective practices for interactions between staff and students. You are encouraged to seek advice from your leadership team if in doubt about the appropriateness of online conduct and report any inappropriate behaviour by colleagues or students.

Online safety risks

- **Sharing too much information –** for example, photos from a party might be OK for close friends to see but could damage a person's **digital reputation** if shared more broadly.
- **Online abuse –** students may behave inappropriately by engaging in online abuse in class online collaboration and LMS platforms. As a staff member, you have oversight of moderating conversations and content, and **reporting that behaviour** where necessary.
- **Image-based abuse –** an intimate image or video of a student could be shared online without their consent, or someone could threaten them over it. Learn more about the risks of **image-based abuse**, which includes **sexual extortion**.
- **Not protecting your own personal information –** account details and location-based information can be used inappropriately by others to physically locate you, source additional information about you or access your online accounts. It is important that you and your students:
  - set **complex passphrases**
  - sign out of platforms when you have finished a class
  - turn off your microphone when you are not talking or need to pause during an online conference or meeting
  - lock your screens when having a break from a class
  - check your settings and take care with the content you share in online platforms or show live on screen, particularly if you are working remotely and multi-tasking – for example, you could be on a webinar and forget to mute your microphone while talking with a family member and accidentally disclose personal information, or someone could see a bill with your home address that's stuck to your fridge if your background is not blurred.

Supporting student safety online

- **Set clear expectations –** share your expectations with students before they start using online platforms for your classes. Let students know what is and isn't acceptable content for sharing and prompt them to stop if they post content that is not relevant to the class. See **Staff use of social media and digital platforms** for an example of a slide that can be used.
- **Remind students** that online learning environments are part of formal learning. Students should be encouraged to always be respectful of one another and adhere to codes of conduct or relevant behaviour policies.
- **Prompt students** about the importance of differentiating between social, academic and professional interactions, including when using online platforms.
- **Use moderation settings** for discussions. These settings can include the option to review all comments prior to being published on a discussion board.
- **Make sure online participants are identifiable** in some manner so that they are unable to post comments anonymously.
- **Share the Tertiary resources hub** with students and colleagues.
- **Remind students that personal information is valuable –** you can provide them with information on how to **protect their personal information.**
- **Encourage students** to think about their **digital reputation** and how they are perceived by others when interacting online.
- **Report breaches of class expectations or institutional policies –** if you see, or have been informed of, inappropriate messages/photos/videos that have been sent on online learning platforms, follow your institution's relevant policies and procedures and flag the issue with the appropriate staff member. eSafety's **collecting evidence** advice can assist in documenting inappropriate content. You can also **report content to eSafety**.
- **Remind students of their options –** if something unacceptable happens online between students, or between students and staff, students can speak to staff or other relevant support services at your institution.

Online learning and collaboration tools

Harmful online behaviour including inappropriate chat and online abuse, image-based abuse and sexual extortion can occur on any online platform. This includes emails, discussion forums and video conference platforms that you use for your classes.

eSafety provides advice on most of the platforms commonly used across universities in **The eSafety Guide**. Make sure that you also refer to your institution's policies and guidance.