Safe use of online collaboration tools

Toolkit for Universities

Creating safer online environments

This resource provides university staff with guidance on how to address online safety issues in the collaboration tools and learning management systems (LMS) used within universities. It aims to help university staff prevent issues such as mistakenly sharing personal information, inappropriate comments being made on discussion forums and system settings which enable anyone to access online tutorials or lectures.

Online learning is becoming more commonplace throughout Australia, with increased use of both online learning and collaboration platforms for classes and group work. In universities, it is important that staff are 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 your university's policies, codes of conduct and other relevant documents which outline staff/student expectations and protective practices staff/student interactions. Staff are encouraged to seek advice from their school, faculty or university leadership team if in doubt about the appropriateness of online conduct and report any unprofessional behaviour from colleagues and students.

Online safety risks

- **Sharing too much information** — for example, photos from a party might be okay for close friends to see, but could damage a person's digital reputation if shared more broadly.
- **Online or cyber abuse** — students may behave inappropriately by engaging in cyber abuse such as sharing offensive material or posting hurtful messages on class online collaboration/LMS platforms. As a class lead you have oversight of moderating conversations and content, and reporting that behaviour where necessary.
- **Image-based abuse** — an intimate image of a student could be shared online without their consent. Learn more about image-based abuse and the risks of sending nudes and sexting.
- **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 strong passwords.
  - 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/ meeting.
  - Lock your screens when having a break from a class.
  - Are mindful of the content you post in online platforms, 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 in person — accidentally disclosing personal information about your location, your partner or other personal information.
- Think about the visual information you send during a video conference. Others on the video call may be able to see objects in the background that can identify where you are — such as street signs or landmarks — or personal information about you like bills or letters pinned to your fridge. Remember, some video conferencing software will allow you to blur the background behind you.

Supporting student safety

You can support the safety of your students in online collaboration and learning tools by:

- **Setting 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 to share and prompt them to stop if they post content that is not relevant to the class.
- **Reminding students** that online learning environments are part of formal university learning. Students should be encouraged to always be respectful of one another and adhere to codes of conduct or relevant behaviour policies.
- **Prompting students** about the importance of differentiating between social and professional interactions, including in online platforms.
- **Using moderation settings** for discussions. These settings can include the option to review all comments prior to being published on a discussion board.
- Making sure online **participants are identifiable** in some manner so that they are unable to post comments anonymously.
- Sharing the **Online Safety 101** toolkit resource with students and colleagues.
- Reminding students that **personal information is valuable** — encourage them not to overshare, and provide them with information on how to protect their personal information.
- **Encouraging students** to think about their digital reputation and how they are perceived by others when interacting online.
- **Reporting** — 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 school or faculty staff. eSafety's collecting evidence advice can assist in documenting inappropriate content. You can also report content to eSafety.
- **Reminding students** that if something unacceptable happens online between students, or between students and staff, students can speak to you, faculty staff or other relevant support services at your university. Speak with staff in your school or faculty so that you have a list of all the relevant contacts and procedures.

Online learning and collaboration tools

Harmful online behaviour including inappropriate chat, cyber abuse and image-based abuse can occur on any online platform used by universities. This includes emails, discussion forums and video conference platforms that you use to run your classes.

eSafety provides advice on most of the platforms commonly used across universities in the eSafety guide. This includes Zoom, Google Hangouts and Meet, Microsoft Teams and Skype. Platforms also offer specific support for educators to assist with online learning. Some of the platforms most commonly used at universities, and links to information about these services, are listed below.

Adobe Connect

- Adobe distance learning resources

Google Hangouts/Meet

- Distance learning for educators training
- Enabling distance learning using Google Meet
- Tips for enabling distance learning through G-Suite and Chrome

Microsoft Teams

- Microsoft Teams help, learning and online classes

Learning Management Systems (LMS)

- Moodle – Learn Moodle basics and Moodle Admin basics
- Canvas – Resources to help with running courses online and video resources
- Blackboard – Remote instruction resources

Published 05/2020