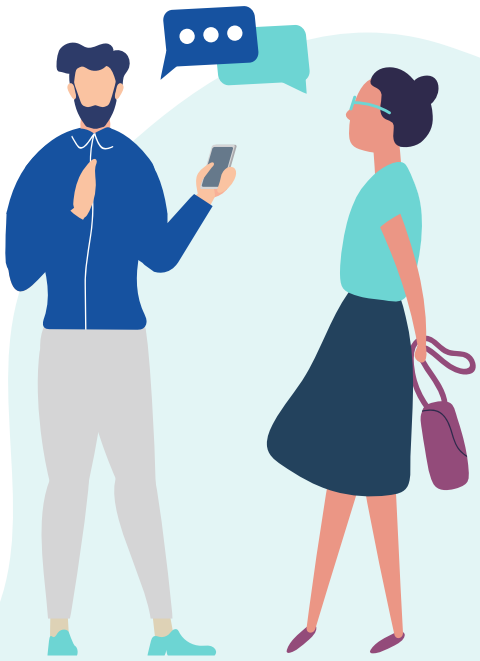
Staff use of social media and digital platforms

Toolkit for Universities

Creating safer online environments



This resource provides guidance for university staff on using social media for professional/university purposes or personal activities. It should be read in conjunction with your university's policies and other relevant documents that outline staff behavioural expectations for social media use, and protective practices for interactions between staff and students.

To ensure a safe and respectful work environment, it is important that all university staff follow policies, procedures and codes of conduct. Staff are encouraged to seek advice from their school, faculty or university leadership team if in doubt about the appropriateness of online conduct and to report any unprofessional behaviour from colleagues/students.

Tips for professional social media use

University staff are encouraged to remember the following tips:

- Communication and content should always reflect professional staff/student relationships.
- Staff should only use university endorsed accounts/ platforms when corresponding with students — avoid using using personal accounts.
- Posts should be positive and professional. Staff are encouraged to avoid personal opinions or views and think twice before posting, noting that it helps to check posts with a trusted colleague for tone and editing.
- Confidential, proprietary or privileged information about other staff, students, research, policies or finances should never be posted or published.
- Student information should not be posted online (including names, videos, photos or work samples) without the written permission of the student.
- If approached by a student with concerns about inappropriate content or misconduct on university social media, staff need to deal with it promptly — following the institution's relevant policies and procedures and flag the issue with the appropriate school or faculty staff member.
- Staff in doubt about professional social media use should ask for guidance from their school, faculty or university executive.

Tips for personal social media use

As a university staff member, you are advised to:

- Maintain professional boundaries on social media and avoid accepting or requesting students as 'friends'. This includes alumni who may still be connected to current students. Have an appropriate response prepared in case a student asks to connect on any social media site.
- Avoid sharing personal mobile numbers or communicating with students using personal social media or email accounts.
- Never exchange personal images with students and avoid storing images or information about students on your personal devices. Never post images of students on personal accounts. Check to see whether your university has a policy about storing student images/information.
- Enable two factor authentication on all social media and email accounts. Avoid logging in to personal accounts on university devices.
- Remember that students and their families can search for staff online, so it is important to consider your personal online presence (including the use of your real name) and to adjust privacy settings as needed. Consider setting up separate accounts for personal and professional use, as well as keeping any personal accounts in private mode.
- Avoid including workplace or work contact details on social media profiles. Listing your university as a place of work on a public social media profile may increase the likelihood of being identified by students. It might also link your personal online profile with the university.
- Check that public interactions (likes, photos, posts) align with the ethos and values of your university. Be aware of guidelines and policies, and model responsible and respectful conduct online.

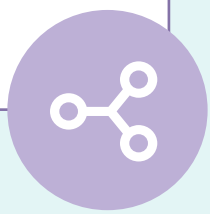
Continued on next page

- Remember that profile pictures are usually visible regardless of privacy settings. Consider deleting old posts and pictures. Deactivate old accounts or request that content is deleted from certain sites if needed, noting that some content may remain public regardless of settings.
- Refrain from posting personal criticisms of colleagues, students and university management online (whether using real names or pseudonyms). Remember that even if a profile is set to private, comments or posts may be visible to others, or copied and passed on — and may be seen as bullying or harassment.
- Avoid using university logos, trademarks or other intellectual property on social media, or making comments on behalf of the university without express consent to do so.

Using social media and online video/collaboration platforms with students

University staff should:

- Be familiar with the university's online safety policies.
- Make online behavioural expectations clear to students at the beginning of class (the slide below offers an example). Share good online safety practices with students — eSafety's responding to cyber abuse guide sets out how to deal with particular types of content. Aim to model good practices also when teaching on digital platforms.
- Learn, and use, online safety skills including how to prevent uninvited attendees from accessing online sessions, how to block video, audio or chat functions, and how to avoid exposing personal information. Make sure you've adjusted the settings for your online classes to protect student safety and privacy and read eSafety's tips on functions and settings to help. Check the eSafety guide for useful links and advice about a range of platforms and services.
- Consider co-designing acceptable use principles with your students at the start of semester — to set expectations for online behaviour.
- Remind 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. Students should also use their student emails and the university's digital platforms to communicate.
- Remind students that if something unacceptable happens online between students, or between students and staff, they can speak to you, faculty staff or other relevant support services at the university. Speak with professional services staff in your school or faculty so that you have a list of all the relevant contacts and procedures. Share good online safety practices with students — eSafety's responding to cyber abuse guide demonstrates good practice.
- Remember not to post examples of student work, exam responses or anecdotes from students without their permission.



Safety in online classes

- Online classes are an extension of the professional learning environment. In both, it is unacceptable to harass, coerce or intimidate others. Online class behaviour is covered by [insert the university's relevant policy/code].
- At [insert university name] we expect that everyone will contribute and demonstrate respectful behaviour towards all other class members online, including academics.
- Examples of respectful behaviour include:
  - Being considerate. This includes not interrupting others while they are speaking and responding when conversation is directed towards you.
  - Being open-minded and listening to others. When you come across ideas you disagree with, focus on responding to the ideas rather than the person who voiced them.
  - Ensuring your language is constructive and doesn't insult or humiliate others.
- If unacceptable behaviour occurs, call it out and access the supports available to you.
- Check out the Toolkit for Universities developed by eSafety and Universities Australia for more information on how to stay safe online, including how to identify and address inappropriate online behaviour.

Published 05/2020