



Staff use of social media and digital platforms



This resource provides guidance for staff on using social media for work purposes or personal activities.

It should be read in conjunction with your institution's policies and other relevant documents which outline expectations for social media use by staff, and best practice for interactions between staff and students.

You are encouraged to seek advice from your school, faculty or leadership team if in doubt about the appropriateness of online conduct and to report any unprofessional behaviour from colleagues and/or students.



Tips for appropriate social media use

- Communication and content should always reflect appropriate staff/student online conduct.
- You should only use accounts/platforms endorsed by your institution when corresponding with students. Avoid using personal accounts.
- Online posts should be positive and appropriate. You should avoid expressing personal opinions or views and think twice before posting or sharing. 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 official platforms, it needs to be dealt with promptly. Follow your institution's relevant policies and procedures and flag the issue with the appropriate person.
- If in doubt about appropriate social media use, you should ask for guidance. Institutions must ensure that the process for seeking help and support is clear to all staff.





Tips for personal social media use

- Maintain appropriate boundaries on social media and avoid accepting or requesting students as 'friends'. This includes alumni (former students) who may still be connected to current students. Make sure you have an appropriate response prepared in case a student asks to connect on any social media platform.
- 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 institution has a policy about storing student images and/or information.
- Enable [two-factor authentication](#) on all social media and email accounts. Avoid logging in to personal accounts on work 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 [digital safety settings](#) as needed. Consider setting up separate accounts for personal and work use, as well as keeping any personal accounts in private mode. You can use [The eSafety Guide](#) to check your privacy settings on the apps you use.
- You may want to avoid including workplace or work contact details on social media profiles. Listing your 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 institution.
- Check any public interactions (likes, photos, posts) align with the ethos and values of your institution. Be aware of any guidelines and policies you must operate within and model responsible and respectful conduct online.
- Remember that profile pictures are usually visible regardless of privacy settings. Consider whether there are any old posts or pictures that should be deleted. You can deactivate old accounts or request that content is deleted from certain platforms if needed, noting that some content may remain public regardless of settings.
- Refrain from posting personal criticisms of colleagues, students and 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 online abuse.
- Avoid posting logos, trademarks or intellectual property of the institution you work for on social media without official consent.
- Avoid making comments on behalf of your institution without official consent.



Using social media and online video/collaboration platforms with students

- Ensure you are familiar with the online safety policies of your institution.
- Remind students that online learning environments are part of their formal learning. Students should be encouraged to be respectful and adhere to codes of conduct or relevant behaviour policies.
- Make online behavioural expectations clear to students at the beginning of the semester or class (the slide included offers an example). Discussing, defining and documenting those behaviours with students can encourage co-ownership and compliance.
- Share [good online safety practices](#) with students. Let them know that eSafety also provides advice about preventing and dealing with [adult cyber abuse](#) and [image-based abuse](#) (sharing or threatening to share an intimate image or video without consent of the person shown).
- Learn how to prevent uninvited attendees from accessing online sessions, how to block video, audio or chat functions, and how to avoid exposing personal information. Check [The eSafety Guide](#) for useful links and advice about a range of platforms and services.
- Advise students to use their tertiary email accounts and the institution's official platforms to communicate with staff members and other students.
- Advise students of the process to follow should unacceptable online behaviour occur between students or between students and staff. This includes outlining who the appropriate people are within the institution that students can report to. Ensure that you have the right contacts and procedures in place.
- Remember not to post examples of student work, exam responses or anecdotes from students without their permission.



An example slide for setting class expectations

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 your institution's relevant policy/code]**.

At **[insert your institution's name]** we expect that everyone will contribute and demonstrate respectful behaviour towards all other class members online, including academics and support staff.

Examples of respectful behaviour include:

- Be considerate. This includes not interrupting others while they are speaking and responding when conversation is directed toward you.
- Be 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.
- Ensure your language is constructive and doesn't insult or humiliate others.

If unacceptable behaviour occurs, call it out and access the supports available.

Check out the [Tertiary resources hub](#) developed by eSafety for more information on how to stay safe online, including how to identify and address inappropriate online behaviour.