



Guide for social media use, video sharing and online collaboration



This guide outlines what to consider when choosing and using social media, video sharing and online collaboration platforms and services on campus.

While social media, video-sharing and online collaboration platforms and services offer many benefits, they also carry risk. To help minimise risks and the likelihood of negative online experiences, aim to use software, digital technologies and online services and platforms with the highest safety, privacy and security standards possible.

You're also encouraged to:

- understand each platform or service and the way personal information is collected, used and stored
- ensure that all technology used complies with relevant legislation, including managing personal information in accordance with the [Privacy Act 1988 \(Cth\)](#) or relevant state and territory legislation
- assess any safety, privacy and security risks before introducing new digital technologies, platforms or services ([eSafety's Risk assessment for introducing new technologies and online platforms resource](#) can help to identify risks.)
- implement measures to mitigate risks, such as actively monitoring and filtering harmful content and using the highest-level privacy settings.

Guidelines



1. Review a platform's or service's safety and privacy settings, community guidelines and terms of use.

- Define how and why your institution will use different technologies, platforms and services. Be clear about the purpose, what is considered acceptable use and what will help to identify and manage potential misuse. Set global content filters and privacy settings. Regularly review and evaluate how technologies are used and refine as needed.

2. Explain to staff (and students where applicable) the uses for social media within the institution.

- The purpose of social media services and platforms is generally to communicate with one another – not to raise complaints about your institution, staff or students. Consider turning off comments and sharing functions to encourage appropriate use. Having clear and transparent internal communication channels will help staff and students to voice their concerns in other ways and seek resolution.

3. Offer teaching staff general guidance about use of online collaboration tools.

- Ensure staff are trained in how to prevent uninvited attendees accessing online sessions, how to turn off video/audio/chat functions and how to avoid exposing personal information. Providing consistent advice on audio-visual and privacy settings for online classes, such as advice on screensharing and blurring backgrounds, will support both teacher and student safety.

4. Determine who will have administration rights and who will be responsible for uploading content and monitoring interactions on platforms or services.

- Ensure accounts have secure login and authentication procedures and are monitored regularly. It is good practice for multiple staff to have administration rights with authority to post on the institution's behalf. It is important to provide targeted training for designated staff.

5. Promote compliance with copyright and trademark laws.

- Advise on acceptable use of the institution's name, logo and brand online and the consequences for misuse. This includes providing guidance to clubs and societies, research and community partners, and the student community. Procedures should be in place to monitor and take down inappropriate posts on official platforms. Referring to potential breaches of copyright or trademarks may help when requesting that content be removed from social media platforms.

6. Respect confidentiality and privacy.

- Seek consent from students and staff prior to publishing personal information online. This includes using:
 - names
 - photos
 - videos
 - work samples
 - other identifying information.
- Consider circumstances that could place a person at risk of harm if their image, video or information is shared, such as where there may be legal proceedings or a court order relating to domestic violence or child protection.
- Recognise that a person's cultural background may be a determining factor in how their names, images and videos can and cannot be used.

7. Consider having an opt in or opt out process for use of personal information.

- Clearly outline what is covered and when extra permissions will be requested. Information published online about a staff member or student should also be taken down if they request its removal.

8. Be clear about managing and storing photos and videos of staff and students.

- This includes where, how and for how long images and videos are stored and the naming conventions used (for easy file retrieval). Securely store consent and media forms as per your Privacy Collection Notice or relevant policy.