Guide for social media use, video sharing and online collaboration

Toolkit for Universities

Creating safer online environments

This guide provides universities with points to consider when choosing and using social media, video sharing and online collaboration platforms.

Disclaimer: This material is general in nature. It is made available on the understanding that the Commonwealth is not engaged in rendering professional advice. Before relying on the material in any matter, you should carefully evaluate its accuracy, currency, completeness and relevance for your purposes and should obtain any appropriate professional advice relevant to your particular circumstances. The Commonwealth does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency or completeness of any material contained in this resource or on any linked site. References to other organisations or websites are inserted for convenience and do not constitute endorsement.

While social media, video sharing and online collaborative platforms can offer many benefits to students, staff and the broader university community they also carry risk. To help minimise risks and the likelihood of negative online experiences universities should aim to use software, online platforms and collaboration technologies with the highest safety, privacy and security standards possible.

Universities are encouraged to:

- understand each platform or service and the way that personal information is collected, used and stored
- ensure that all technology used within the university 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 social media services to the university — eSafety's Toolkit resource: Risk assessment introducing new technologies and online platforms 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 or service's safety and privacy settings**, community guidelines and terms of use. Define how and why your university will use different technologies and platforms. 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**, that the purpose of social media services and platforms is to communicate with one another — not to raise complaints. Consider turning off comments and sharing to encourage appropriate use. Clear and transparent internal communication channels within the university 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 block 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 further support teacher and student safety. eSafety has some general tips about online collaboration that complement this learning.

4. **Determine who will have administration rights** and who will be responsible for uploading content and monitoring interactions on sites or platforms. Accounts should have secure login and authentication procedures and be monitored regularly. It is good practice for multiple staff to have administration rights, but it is important that all administrators have the authority to post on the university's behalf. Universities are encouraged to provide targeted training for these staff.

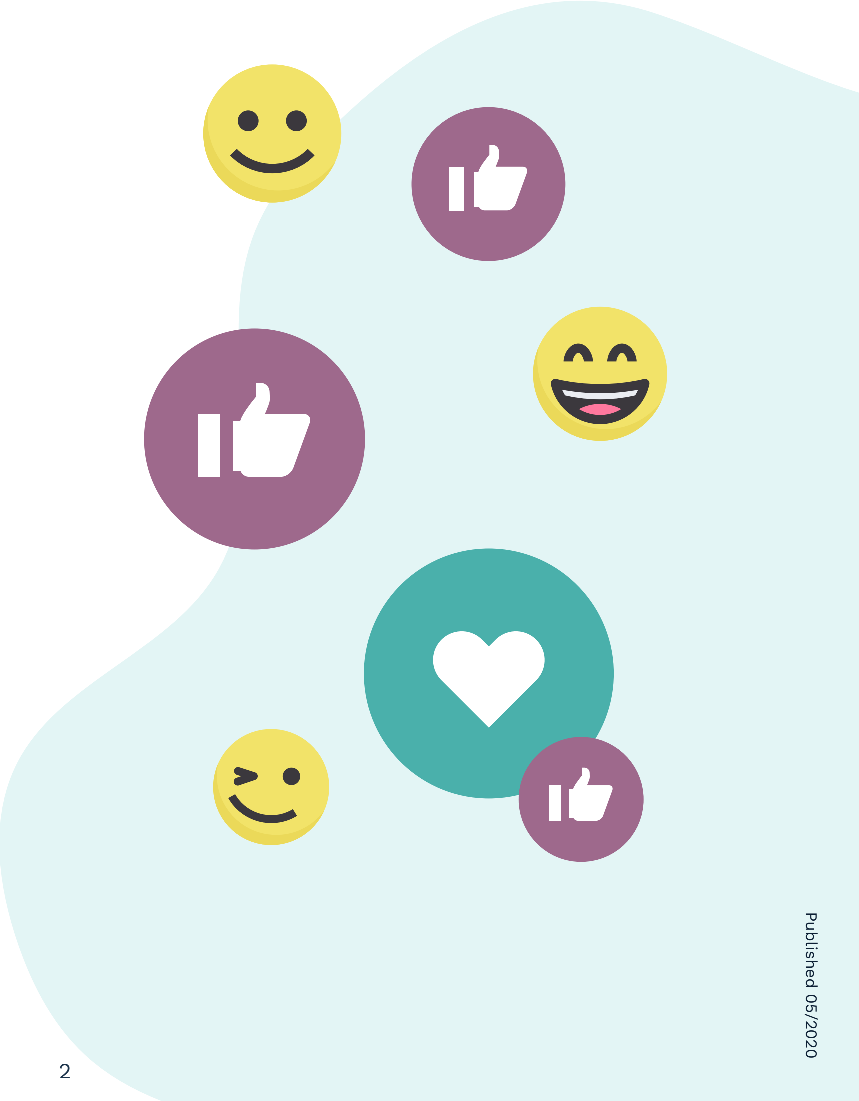
5. **Promote compliance with copyright and trademark law** by advising the university community about acceptable use of the university's name, logo and brand online and the consequences for misuse. This includes providing guidance to clubs and societies, research and community partners, and the student community. Procedures should be in place to monitor and take down inappropriate posts on university sites. Referring to potential breaches of copyright or trademarks may help when requesting that content is removed from social media sites.

6. **Respect confidentiality and privacy** by always seeking consent from students and staff prior to publishing information online. This includes names, photos, videos, work samples or other identifying information. Universities could consider having an opt in or opt out process that clearly outlines what is covered and where extra permissions will be requested.

   Any information published online about a staff member or student should be taken down if requested by the person it concerns.

7. **Be clear about managing**, **storing and sharing photos/videos** of staff and students. This includes where, how and for how long images are stored and the naming conventions used with images. Securely store consent and media forms as per your Privacy Collection Notice or relevant policy.

   Recognise that a person's cultural background may be a determining factor in how their images can and cannot be used. Consider circumstances that could place a person at risk of harm if their image or information is shared, such as where there may be legal proceedings or a court order relating to domestic violence or child protection.



Published 05/2020