



Tips for staff using social media

Creating safer online environments



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 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.

Why was this guide produced?

This tip sheet provides guidance for school staff on using social media for:

- professional use for approved school-related purposes
- classroom use in line with social media age restrictions, including video sharing and online collaboration platforms
- personal use.

This guide can be read in conjunction with [Prepare – Guidelines for social media use, video sharing and online collaboration](#). It should also be read alongside relevant school and/or education sector policies and procedures that set out professional standards and codes of conduct.

Please note: Under-16s are still allowed to see publicly available social media content that doesn't require logging into an account.

Tips for professional social media use

- At school, social media is best used solely for educational purposes. Communication modes and content selection should reflect professional standards of behaviour and should adhere to the social media minimum age.
- Staff should use only school-authorized social media accounts and platforms when corresponding with parents/carers. Avoid ever using personal accounts.
- At least two members of staff should have access to school-authorized social media accounts, including a member of the school leadership team. These staff will be responsible for uploading content and monitoring and moderating audience interactions. Schools are encouraged to provide training and support for these staff members.
- Posts to school social media accounts should be positive and professional. It is important to be mindful of what is posted and the audience you are connecting with. Check in with a trusted colleague to help with tone and editing.
- Note that students and parents/carers may search for staff social media profiles online, so it is important to consider your personal online presence (including the use of your real name) and to tighten privacy settings. For information on social media platform privacy settings see the [eSafety Guide](#).
- Confidential, proprietary or privileged information about staff, students, parents/carers, or school projects, policies or finances should never be posted or published.
- Student personal information should not be posted online (including names, videos, photos or work samples) without the written permission of the school, student and parent/carer.
- If approached by a student or parent/carer with concerns about inappropriate content or misconduct on school social media, staff need to deal with it promptly, following school and/or education sector policies, where applicable.
- Staff in doubt about professional social media use should ask for guidance from a school leader.
- Remember that sometimes profile pictures can be visible regardless of privacy settings. Consider deleting old posts and photos. Deactivate old accounts and request that content is deleted from certain sites if needed, noting that some content may remain public regardless of settings.
- Refrain from criticising your education sector, school management, colleagues, students, their parents/carers, 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 and may be copied in screenshots and shared.

Tips for professional social media use, cont.

- Avoid including workplace contact details such as email addresses or telephone numbers on social media profiles. Listing your school as a place of work on a social media profile that is public may increase the likelihood of being identified by students and parents/carers.
- Be aware of guidelines and policies set by employers and model responsible and respectful conduct online.
- Avoid using school logos, trademarks or other symbols that have intellectual property implications on social media or making comments on behalf of the school without consent to do so.

Tips for classroom social media use, video sharing and online collaboration platforms

Staff need to:

- Be familiar with the school's online safety and mobile device usage policies, including those linked to the [social media minimum age restrictions](#).
- Make online behavioural expectations clear to students. Teach students online safety skills and communication protocols. Model good practice when using technology in the classroom.
- Consider co-designing acceptable use agreements with students to set expectations for online behaviour. eSafety's [Online Safety Classroom Agreement](#) can be a starting point.
- If a student is undertaking a presentation in class, remember to preview PowerPoint slides, images, videos, website links, beforehand to check for appropriateness.
- Refrain from posting examples of student work, exam responses or anecdotes from students without consent from the student and parent/carer.
- Preview social media content for appropriateness and ensure it is approved by school leadership when using social media in your classroom.

Tips for personal social media use

- Maintain professional boundaries on social media and avoid accepting or extending 'friend' or connection requests to students or parents/carers. This includes former students who may still be connected to current students at the school – for example, through tutoring or coaching. Be prepared with an appropriate rehearsed response when a student or parent/carer asks to connect with you on social media, gaming or other platforms.
- Avoid ever sharing personal mobile numbers and communicating with students and parents/carers using personal social media and email accounts.
- Never exchange personal images with students via text messages and avoid storing images of, or information about, students on personal devices. Never post images of students on personal accounts. Check to see whether there are sector guidelines and infrastructure requirements for storing student images on school and/or education sector networks.
- Enable two factor authentication on all social media and email accounts. Avoid ever logging into personal accounts on school devices or using personal devices during class time.
- **Remember:** if you can't avoid logging in, make sure you log out of your accounts each time these are used.