



# Guidelines for social media use, video sharing and online collaboration

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 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.

These guidelines support schools' use of social media, video sharing and online collaboration platforms. Policies and procedures should be consistent with, and informed by, school and/or education sector policies and procedures.

Please note that from 10 December 2025, age-restricted social media platforms will have to take reasonable steps to prevent Australians under the age of 16 from creating or keeping an account. Please refer to eSafety's social media age restrictions hub.

Using social media for communicating with parents and carers, and video sharing and online collaborative platforms in learning and teaching is common practice in some school communities. However, this use also carries risks. Schools should endeavour to use products with the highest safety, privacy and security standards possible.

## Guidelines

**1. Ensure use of the platform is authorised** by the education sector and/or school leadership team before setting up school social media accounts for parents/carers. Schools should comply with existing policies when setting up and managing these accounts.

**2. Review the platform's safety and privacy settings, community guidelines and terms of use** and define how and why the school will use different technologies and platforms. Being clear about the purpose, and what is considered acceptable and unacceptable use, will help to identify and manage potential misuse. Schools should regularly review and evaluate how technologies are used and refine as needed.

**3. Communicate to the school community** that the purpose of school social media is to share school communications, not to raise complaints. Consider turning off comments and disabling post sharing to encourage appropriate use. For example, some platforms give administrators the option to disable features on individual posts or adjust the default settings for all posts. Schools are encouraged to have clear and transparent communication channels to enable students and parents/carers to voice their concerns, make complaints, and seek resolution through these channels rather than on social media.

**4. Determine who will have administration rights** and who will be responsible for uploading content and monitoring interactions on sites or platforms. School accounts should be monitored regularly and have secure login and multifactor authentication procedures. It is good practice for at least two members of staff to have administration rights, plus a member of the school leadership team. Schools are encouraged to provide targeted training and support for these staff members. Moderation may need to be scheduled outside work hours.

**5. Promote compliance with copyright and trademark law** by advising the school community about acceptable use of the school's name, logo and brand online and the consequences for misuse. Procedures should be in place to monitor and take down inappropriate posts on school social media sites. Referring to potential breaches of copyright or trademarks may help when requesting that content is removed from social media sites. See the [eSafety Guide](#) for specific information about terms of use.

**6. Respect privacy and autonomy** by always seeking consent from students, parents/carers and staff before publishing their personal information online. Personal information includes name, date of birth, phone number, school name, location, student ID, IP address, images and biometrics (e.g. facial recognition).

Permission can be obtained through an annual blanket consent form for regular communications such as newsletters, with specific consent requested for special events and unscheduled communications. Provide information on the possible use of student images to enable parents/carers and students themselves to have a clear understanding of what they are consenting to, and who will have access to images and/or information.

**7. Be clear about managing, storing and sharing photos and videos** of students and other school community members. This includes where, how and for how long images are stored, the naming conventions used with images and videos and whether the school permits students and parents/carers to record events. Securely store consent and media forms as per the school's Privacy Collection Notice or school privacy policy, ensuring this is in line with the school and/or education sector policy.

Ensure that concerns from students and parents/carers about the use of images and videos are taken seriously and responded to promptly and thoroughly, and that complaint handling processes are understood by students, parents/carers, and school staff.

Recognise that a student's cultural background or other circumstances may be a determining factor in how their images can and cannot be used. Consider circumstances that could place the student 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 child protection, custody, domestic violence or family separation.

**8. Schools are also encouraged to:**

- understand the technology and the way that personal information will be collected, used and stored
- ensure the technology complies with relevant legislation, including managing personal information in accordance with the [Privacy Act 1988 \(Cth\)](#) and relevant state and territory legislation, as well as any applicable department or sector policies
- assess privacy and security risks before introducing new digital technologies or learning platforms to the school. Learn more in [Prepare 3 - New technologies risk-assessment tool](#)
- implement measures to mitigate risks, such as actively monitoring and filtering harmful content and using the highest-level privacy settings.