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

## eSafety Toolkit for Schools

Creating safer online environments

**These guidelines support the safe use of social media, video sharing and online collaboration platforms in schools. Policies and procedures should be consistent with, and informed by, education department or sector policies and procedures.**

Using social media, video sharing and online collaborative platforms in schools can benefit students and the broader school community. However, it also carries risk. Schools should endeavour to use software, online products and collaboration technologies with the highest safety, privacy and security standards possible.

**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.

CC BY NC SA

## Guidelines

1. **Ensure use is authorised** by the education department or sector and school leadership team before setting up a school social media account. Schools should comply with existing departmental or sector policies, privacy and copyright when setting up and managing the account.

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 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 sites and platforms is to share school communications — not to raise complaints. Consider turning off comments and sharing on posts to encourage appropriate use. Schools are encouraged to have clear and transparent communication channels within the school (not on social media) to enable students and parents/carers to voice their concerns and seek resolution.

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 have secure login, authentication procedures and be monitored regularly. It is good practice for at least two members of staff to have access, including a member of the school leadership team. Schools are encouraged to provide targeted training for these staff.

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 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 the student and their parent/carer, and staff consent, prior to publishing their information online. This includes names, photos, videos, work samples or other identifying information. Schools could have an opt in or opt out process at the start of each year that clearly outlines what is covered and where extra permissions will be requested.

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 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 local policy, ensuring this is in line with the education department or sector policy.

   Recognise that a student's cultural background 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) or relevant state and territory legislation, as well as any applicable department or sector policies
   - assess any safety, privacy and security risks before introducing new digital technologies or social media 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 setting the highest level privacy settings.

Updated 09/2022