# CYBERSAFETY AND RESPONSIBLE USE OF DIGITAL TECHNOLOGIES

## POLICY

This policy outlines measures schools must take to support students to engage with digital technology in a safe and responsible way.

## SUMMARY

- Schools have a duty of care to students to take reasonable steps to ensure digital learning is conducted in a safe and responsible manner.
- Schools must ensure students are aware of expectations relating to the safe, responsible and ethical use of digital technologies. The Department has developed acceptable use agreement templates, to support schools with this requirement.
- Online safety should be included in curriculum planning.
- Online incidents of concern must be managed in accordance with the Department's policy on Reporting and Managing School Incidents, as well as any other Department or local school policy relevant to the type of incident.

## DETAILS

Schools must ensure that digital learning is conducted in a safe and responsible manner by staff and students and the use of online environments is for educational purpose, is appropriate and balanced. Schools also have a responsibility to educate young people about responsible online behaviour.

To manage risk and support the safe and responsible use of digital technologies, the following areas need to be considered when planning for digital learning.

## SUPERVISION WHEN USING DIGITAL TECHNOLOGY IN THE CLASSROOM

Consistent with their duty of care to students, teachers are required to adequately supervise students when using digital technology in the classroom. Schools should have measures in place to ensure students are appropriately supervised when engaged in online learning. Such measures might include:

- moving around the room to regularly monitor screens
- installing remote access software that enables teacher access to individual students' 1 to 1 learning device used in class
- actively reinforcing learning and behavioural expectations during the activity

Further information about supervision of students more generally, is available at Supervision of Students.

Further information explaining the duty of care owed by school staff towards students can be found at Duty of Care.

## STUDENT ONLINE BEHAVIOUR EXPECTATIONS: ACCEPTABLE USE AGREEMENT

Schools must ensure students are aware of behavioural expectations when engaging in digital learning activities.

The Department has provided Acceptable Use Agreement (AUA) templates (refer to the Resources tab) to assist schools to develop agreements around the acceptable use of internet, other online and digital technologies. Whilst not legal documents, they play an important part in describing how the school educates and supports its students as well as the expectations on students themselves to be safe, responsible and ethical users of digital technologies.

These agreements are templates. Schools can add and/or delete information where necessary to make them relevant to their school environment. It is recommended that teachers work through and discuss the

behaviours described in the agreement with their students. Inclusion of student voice in the AUA can assist with addressing relevant issues and share knowledge of current technologies and social media sites. The AUA must be accurate, communicated across the community and reviewed regularly. Sending a copy of the AUA home or publishing it on the school website will assist parents to support their child's appropriate internet use at home.

Schools may also wish to recommend that parents discuss, develop and implement a similar 'family agreement' at home. This will assist students to understand what is and isn't appropriate behaviour and that appropriate behaviour is expected everywhere and anytime they are online.

When developing their AUA, schools must:

- ensure the safe and responsible use of digital technologies is the paramount consideration
- ensure that their AUA is consistent with their school student engagement policy
- add information about programs, online and digital technologies including social media tools specific to their school
- describe strategies designed to teach students to be safe, responsible and ethical users of digital technologies when they are not at school
- provide information to parents and/or carers about the AUA, the school's programs and considerations for at-home use of online and digital technologies
- retain a copy of the completed and signed AUA on file at the school

Refer to the Resources tab for AUA templates and guidelines, tailored for a range of student age groups.

Schools are reminded that students' signing of these agreements is aimed to raise awareness and support student learning. They are not legally binding on those students. There are however some online activities which are illegal and schools are required to report these to appropriate authorities.

## PRIVACY IN ONLINE ENVIRONMENTS

All school and corporate staff must take reasonable steps to ensure that personal and health information they create, handle or have responsibility for are kept secure at all times, and only collect, use and disclose it in appropriate ways. Refer to: Privacy and Information Sharing.

Online services and applications, including cloud technologies, often handle student or parent information. These services usually require personal details to create an account or 'login' and often also provide an opportunity for personal information to be created or stored within the software by a teacher and/or student.

**Privacy impact assessments**

When schools are considering using an online service or application that handles personal information they must:

1. Obtain agreement to do so from the school principal or leadership team. This can be done via email or a meeting.
2. Conduct an assessment to identify any privacy and security risks, and document what actions are required to mitigate these.
3. Consider whether consent for use of the service is required, and if so, whether opt-in or opt-out consent is most appropriate for the specific situation.
4. Ensure parents are adequately informed about the use of the online service.

When schools start new initiatives or plan to use new or updated systems that handle personal, sensitive or health information, a privacy impact assessment (PIA) is required.

For guidance, tools and a template for conducting a PIA, as well as further information on parent consent refer to Privacy and Information Sharing.
For advice on Departmentally brokered services and applications, contact the Digital Learning Unit at digital.learning@education.vic.gov.au

For further privacy advice and support, contact the Privacy team privacy@education.vic.gov.au

## DIGITAL COPYRIGHT

Digital material on the internet is protected by copyright in the same way as other copyright works. The material that comprises a website may be owned by different people. For guidance on copying and communicating digital material, refer to the Smartcopying digital teaching environment manual.

For information on how to use digital and other material produced by the Department and students, refer to: Intellectual Property and Copyright.

For copyright advice, contact the Copyright team at copyright@education.vic.gov.au

## POSTING PHOTOGRAPHS ONLINE

When including photographs of students in online platforms and applications, it is important to consider risk and consent. Refer to: Photographing, Filming and Recording Students.

## CYBERSAFETY EDUCATION

Online safety education should be included within the school's curriculum planning and taught explicitly.

- Bully Stoppers — supports students, parents, teachers and principals in working together to make sure schools are safe and supportive places
- classroom resources — links to downloadable classroom activities, videos, interactive learning modules and quiz, advice sheets and other useful resources to use in the classroom
- eSmart — assists schools to develop a culture that promotes the safe, smart and responsible use of technology
- the eSafety Commissioner — the office provides a range of up-to-date information and resources, coupled with a complaints system to assist children who experience serious cyberbullying and image-based abuse

For more information, contact student.engagement@education.vic.gov.au

## RESPONDING TO ONLINE INCIDENTS

Schools must respond to any online incident in accordance with the Department's policy on Reporting and Managing School Incidents, as well as any other Department or local school policy relevant to the type of incident, such as the school's student engagement and bullying prevention policies, or the Department's Privacy and Information Sharing policy and associated guidance.

For information on managing cyberbullying specifically, refer to:

- Bullying Prevention and Response
- Bully Stoppers
- Student Engagement

For online incidents, the Department has also developed a step-by-step guide, which provides practical steps and actions to respond to an online incident of concern:

- Step-by-step guide for responding to online incidents of inappropriate behaviour by students

This guide is also available on the Resources tab.

## STUDENTS USING MOBILE PHONES

From Term 1, 2020, students who choose to bring mobile phones to school must have them switched off and securely stored during school hours unless an exception has been granted.
For more information on this policy, including when exceptions may be granted, refer to: Mobile Phones — Student Use.

## WORKING WITH PARENTS

Parents and/or carers have an important role in helping their children use digital technologies safely and responsibly. Schools can assist parents to support their children in the digital world by providing them with useful information about existing and emerging technologies, engaging them in the development and review of policies and inviting them to information sessions or distributing handouts on school expectations of acceptable use.

Schools also have a responsibility to inform parents and/or carers of any learning spaces that they make available to students as well as the expected behaviours and protocols surrounding their use.

**Parent information sessions**
Parent information sessions should focus on the safety and wellbeing implications of online environments in addition to any technical details parents might need to know to support their child at home. Information evenings can raise parent awareness about the safe and responsible use of digital technologies and provide parents with ideas about measures that could be taken at home.

While school and home environments may not be exactly alike, schools can still promote general safety strategies and ease parental concerns. To this end, schools might find their student engagement and bullying prevention policies and acceptable use agreements useful starting places for discussion.

## SCHOOL POLICY ON DIGITAL TECHNOLOGIES AND THE INTERNET

Schools must have a local policy that addresses the use of digital technologies and the internet in their school. A template Digital Technologies (Internet, Social Media and Digital Devices) is available on the School Policy Templates Portal (login required). Schools can modify the template to suit their local circumstances.

## DEFINITIONS

**Cyberbullying**
Direct verbal or indirect bullying behaviours using digital technologies. This includes harassment via a mobile phone, setting up a defamatory personal website or deliberately excluding someone from social networking spaces.

## RELATED POLICIES

- Bullying Prevention and Response
- Digital Learning in Schools
- Duty of Care
- Mobile Phones — Student Use
- Privacy and Information Sharing
- Reporting and Managing School Incidents (including emergencies)
- Social Media Use to Support Student Learning
- Student Engagement

## RELEVANT LEGISLATION

- Education and Training Reform Act 2006 (Vic)
- Privacy and Data Protection Act 2014 (Vic)

## EVALUATION

This policy is taken directly from the Department of Education and Training's Policy and Advisory Library (PAL) dated **October 8, 2021** and will be reviewed in line with new legislation, regulations and best practice.

## POLICY REVIEW AND APPROVAL

| | |
|---|---|
| Policy last reviewed | January 2022 |
| Consultation | Leadership<br>School Council |
| Approved | February 2022 |
| Next scheduled review date | January 2023 |