



CYBER SAFETY POLICY

Mitcham Primary School

PURPOSE

This policy outlines measures schools must take to support students' safe and responsible use of digital technology.

SCOPE

- 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.

POLICY

The school will ensure that digital learning is conducted safely and responsibly by staff and students, and the use of online environments for educational purposes 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 TECHNOLOGIES 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 teachers access to individual students' 1 to 1 learning devices used in class
- actively reinforcing learning and behavioural expectations during the activity

STUDENT ONLINE BEHAVIOUR EXPECTATIONS: ACCEPTABLE USE AGREEMENT

Our school ensures that students are aware of behavioural expectations when engaging in digital learning activities.

Students' signing of these agreements is aimed at raising awareness and supporting student learning. They are not legally binding on those students. There are however, some online activities that are illegal, and schools are required to report these to the 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 is 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 at 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.

- [The Cyber Safety Project](#) – Empower schools and families to navigate the online world safely through carefully planned lessons and sequences for students in F-6
- [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, 2025, 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. Multiple yearly webinars run by [The Cyber Safety Project](#) 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.

FURTHER INFORMATION AND RESOURCES

- [Education and Training Reform Act 2006 \(Vic\)](#)
- [Privacy and Data Protection Act 2014 \(Vic\)](#)

Policy Review and approval

Policy last reviewed	August 2025
Approved by	Principal
Next scheduled review date	August 2027