



ICT Acceptable Use Standard

Last Updated: 29 July 2025

The following policy should be read in conjunction with the [Behaviour Policy](#).

Preamble

The measures to ensure the cyber-safety of students at Mitcham Primary School are based on our core values. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this document.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at Mitcham Primary School, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school, and used on or off the site.

The overall goal of Mitcham Primary School is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. This standard includes information about your child's obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

Material sent and received using the network may be monitored and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail. Where a student is suspected of an electronic crime, this will be reported to the South Australian Police. Where a personal electronic device such as a mobile phone is used to capture images of a crime, such as an assault, the device will be confiscated and handed to the police.

While every reasonable effort is made by schools and the Department for Education (DfE) administrators to prevent children's exposure to inappropriate content when using the department's online services, it is not possible to completely eliminate the risk of such exposure. In particular, the DfE cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. The DfE recommends the use of appropriate Internet filtering software.

More information about Internet filtering can be found on the websites of the Australian Communications and Media Authority <http://www.acma.gov.au>, NetAlert <http://www.netalert.gov.au>, the Kids Helpline <http://www.kidshelp.com.au> and Bullying No Way <http://www.bullyingnoway.com.au>.

Please contact the principal if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.

Important terms

Cyber-safety refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

Cyber-bullying is bullying which uses technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as email, chat room discussion groups, instant messaging, web pages or SMS (text messaging) - with the intention of harming another person.

School and preschool ICT refers to the school's or preschool's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.

ICT equipment/devices includes computers (such as desktops, iPads, tablets, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other similar technologies.

Inappropriate material means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school or preschool environment.

E-crime occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

Strategies to help keep Mitcham Primary School Students Cyber-safe

Parents/Caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices. Being cyber-safe is no exception and we invite you to discuss with your child the following strategies to stay safe when using ICT during and out of formal school hours.

Student Declaration

- I will use the school's computers and other ICT equipment only for my learning.
- I will go online or use the Internet at school only when a teacher gives permission and an adult is supervising.
- I understand that my Internet and email access is filtered and monitored by Mitcham Primary School and the DfE.
- I will log on only with my user name. I will not allow anyone else to use my login details.
- I will keep my password private.
- I will use the Internet, email, or any ICT device only for positive purposes, not to be violent, mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school.

While at school, I will:

- only attempt to search for things online that I know are acceptable at our school. This would exclude anything that is violent, mean, rude or offensive, or that I know our school finds unacceptable.
- report any attempt to get around or bypass security, monitoring and filtering that is in place at our school.
- not attempt to install or run software other than what is already installed on school devices.
- not attempt to use online services or systems outside those provided by the DfE / LearnLink Office 365 that store my information such as Seesaw, Class Dojo, Makers Empire, Unity, Dropbox etc. without prior written permission given
- from my parent/caregiver to Mitcham Primary School.

If I find anything that upsets me, is obscene, violent, threatening, mean or rude, or that I know is not acceptable at our school, I will:

- not show others
- turn off the screen (or minimise it)
- report it to a teacher straight away.

I understand that students are discouraged from bringing mobile phones to school. Other personal ICT devices including laptops, iPads, tablets etc. are not permitted at school. I will not attempt to connect to the school's network (via Wi-Fi or other means) with any device that I bring to school.

I understand that mobile phones at school belonging to students are to be switched off, placed in cases and kept in front office during school hours. I understand that mobile phones are not to be used during the school day and are collected from the front office at the end of the day. I understand that the school cyber-safety strategies apply to any device brought to school.

I will ensure my compliance with copyright laws, by downloading or copying any files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material.

I will not put any personal information online. This includes any personally identifying information including any of the following:

- my full name
- my address
- my email address
- my phone numbers
- photos of me or other people
- identifiable photos that are associated to Mitcham Primary School

I will not email or share photos or images of myself or other people without prior permission from a teacher.

I will respect and will treat all ICT equipment/devices with care. This includes:

- Not intentionally disrupting any school ICT systems
- Not attempting to gain unauthorised access to or “hack” any system
- Respecting the privacy of other people’s data
- Following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICTs
- Reporting any breakages & damage to a staff member immediately.

I know that if I do not follow cyber-safety practices the school may inform my parents/caregivers. In serious cases, the school may take disciplinary action against me. My family may be charged for repair costs. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold personal items securely for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

I have read and understand the LearnLink Office 365 information in [Appendix A](#) and accept that the LearnLink Office 365 services including Office 365 ProPlus is only to be used in relation to my learning. I will not use LearnLink Office 365 to store the personal information of others and myself. I will keep my device updated and protected from viruses & malware and do a complete backup of the device before the installation of Office 365 software. I will also ensure I have my data securely backed-up should the LearnLink Office 365 service not be available. I understand and accept the risks of using the LearnLink Office 365 service.

Policy update and review

The school council and staff regularly monitor and review the effectiveness of the Student ICT Acceptable Use Standard (at least every three years) and revise the policy when required.

Policy last reviewed May 2023. Next review May 2026.