



Digital Citizenship Policy

Purpose

Mid North Christian College aims to embed a digital learning culture with clear policies and guidelines, which provides guidance to staff, students, parents and others about what constitutes a safe, respectful and caring environment where technologies are used smartly, safely and responsibly for learning and communicating. This is in keeping with the College's Vision and Mission, our legislative and professional obligations, and the community's expectations. Within this context, the object of this policy and guidelines statement is to ensure the smart, safe, responsible and ethical use of technology within the College's community. Mid North Christian College views digital citizenship as a shared responsibility between students, parents and the College.

At Mid North Christian College, we:

- Recognise that the internet and digital technologies are valuable teaching and learning devices which need to be used responsibly and sensibly.
- Provide access to devices in all year levels with Secondary students given their own device to use at home as well as at school.
- Have clear policies in place around expected behaviours when students are using digital technology and the internet.
- Support students to develop digital literacy skills within an educational environment
- Have a digital citizenship program in the College.
- Use an array of technologies for educational purposes.
- Provide a filtered internet service for computers logged into the College's network. Parents need to provide filtering and supervision of use on the student's home network.

Obligations and Requirements Regarding Use of ICT in the College's Learning Environment

1. Student Responsibilities

Respect and Protect Themselves and Others.

Users must:

- Show respect to the College's ICT devices they use, maintaining the device in good working order, free from damage and without tampering, not attempting to tamper with the original configuration of any software or hardware.
- Not attempt to circumvent the College's internet filtering facility, this includes tethering phones (hot spotting e.g. using phones to access the internet).
- Not allow other students to use a device assigned to them.
- Show respect for themselves through their actions. Select online names that are appropriate and consider the information and images that they post online and not disclose their, or anyone else's personal details.
- Ensure that the information, images and materials posted online will not put them at risk.
- Report any attacks or inappropriate behaviour directed at them and seek support from a trusted adult or organisations.
- Protect passwords, accounts and resources.
- Ensure any profiles and related content is consistent with how they wish to present themselves to their parents/caregivers, peers and wider community and is in line with the College's Visions and Mission.

- Protect others by reporting abuse, not forwarding inappropriate materials or communications; and not visiting sites that are degrading, pornographic, racist or inappropriate.
- Moderate unacceptable materials and conversations, and report conversations that are inappropriate or unacceptable.
- Show respect to others and not use electronic mediums to bully, harass or stalk other people.
- Ensure that the information, images and materials posted online will not put others at risk.

2. Parent/Caregiver Responsibilities

- Ensure their child is using their College issued device appropriately while at home.
- Ensure the College device remains in good working order free from wilful damage while at home.
- Is responsible for any damage caused to the device that is not covered by the College's insurance.
- Encourage their child to act responsibly and support them to understand our College's policies.
- Keep track of their child/ren's online use when they are not at the College – including mobile apps, online games, and other social media.
- Talk to their child/ren about what is – and is not – acceptable online behaviour.

3. Staff Responsibilities

- Must abide by all policies and standards surrounding Information, Communication Technology (ICT) and child safety as outlined by the College and the Association of Independent Schools in South Australia (AISSA).
- Help students learn how to act when working online with others.

Operational Aspects

1. Requirements regarding appropriate use of ICT at Mid North Christian College

In order to meet the College's legislative obligations to maintain a safe learning environment, and to uphold the values of Mid North Christian College:

- The use of Mid North Christian College's computer network, internet access facilities, computers and ALL school equipment/devices, on or off the College site, is limited to educational purposes as appropriate to the College environment. This applies whether the ICT equipment is owned by the user or is owned by the College. Any exception to this requirement is solely at the discretion of the College.
- Mid North Christian College has the right to monitor, access, and review all the use detailed above. The College can use any means it chooses to ensure appropriate use of ICT devices and the College network. This includes personal emails sent and received on the College's computers and/or network facilities, either during or outside College hours. The College maintains the right to lock/disable/remove/modify domain/local computer accounts where deemed appropriate at its sole discretion.
- The use of any privately or College owned ICT equipment/devices on the school site, or at any College-related activity come under the same usage expectation. This includes any images or material present/stored on privately-owned ICT equipment/devices brought onto the College site, or to any College-related activity. Any person unsure about whether it is appropriate to have a particular device at Mid North Christian College or at a College-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the Mid North Christian College's ICT Coordinator. Note that examples of a 'College-related activity' include, but are not limited to, a field trip, camp, sporting or cultural event, *wherever* its location.
- Despite our best efforts, when using a global information system such as the internet, it may not always be possible for the College to filter or screen all material. This may include material which is **inappropriate** in the College environment (such as 'legal' pornography), **dangerous** (such as sites for

the sale of weapons), or **illegal**. The expectation is that each individual will make responsible use of such systems. In the event of such use, students must be able to demonstrate their connection to current classroom learning.

Every individual is to be accountable for the responsible and appropriate use of ICT.

Definitions

Parent: is interchangeable with “care-giver”.

Social Media: includes the various online technology tools that enable people to communicate easily via the internet to share information and resources. Social media can include text, audio, video, images, podcast and other multimedia communications. It includes, but is not limited to websites such as Twitter, YouTube and Facebook.

ICT: refers to the term ‘Information and Communication Technologies’.

Cybersafety: refers to the safe use of the internet and ICT equipment/devices, including mobile phones.

School ICT: refers to the College’s computer network, internet access facilities, computers, and other College ICT equipment/devices. This also includes subsidiary or public organisation(s) equipment which may extend and/or be part of the College network infrastructure.

ICT equipment/devices: includes but it is not limited to, computers (such as desktops, laptops, iPads), storage devices (such as USB and flash memory devices, CDs, DVDs, iPads, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers, gaming devices and any other, similar, technologies as they come into use.

Users: all students that have access to Mid North Christian College’s ICT systems with username and password.

Network: all internally controlled infrastructure that connects user hardware devices to each other and to information.

Security: measures put in place to protect the systems and information contained within the systems.

Resources

www.cybersmart.gov.au

www.bullyingnoway.gov.au

www.cybersafety.communications.gov.au/resources/education

Australian Communications and Media Authority

END OF POLICY

Authorisations

Other related documents: Child Safe Environments Policy, MNCC Child Safety Code of Conduct, IT User Agreements for Primary and Secondary Students, Use of Social Media Policy

Policy Reviewer: Principal - Rachel Richardson

Approval by: Board

Board Approval required: Yes

New or Revised Policy: New

Approved date of Policy: 31/8/23

Next Review date: End of 2025

Last Updated: RR 22/7/23