

DIGITAL CITIZENSHIP POLICY

Torrens Valley Christian school aims to embed a digital learning culture with clear policies and guidelines, in line with our Vision and Values statement, 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 School's Vision and Values, 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 School's community. The School views digital citizenship as a shared responsibility between students, parents and the School.

At Torrens Valley Christian School 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 School 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 School.
- Use an array of technologies for educational purposes.
- Provide a filtered internet service for computers logged into the school's network. Parents may need to provide filtering and supervision of use on the student's home network.

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

1. Student Responsibilities

Respect and Protect Themselves and Others.

Users must:

- Show respect to the school'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 school'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 schools Vision and Values.
- 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 your child is using their school issued device appropriately while at home.
- Ensure the school device remains in good working order free from willful damage while at home.
- Is responsible for any damage caused to the device that is not covered by the school's insurance.
- Encourage your child to act responsibly and support them to understand our school's policies.
- Keep track of your child/ren's online use when they are not in school – including mobile apps, online games, and other social media.
- Talk to your 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 located as outlined by the School 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 Torrens Valley Christian School

In order to meet the School's legislative obligations to maintain a safe learning environment, and to uphold the values of Torrens Valley Christian School:

- 1.1. The use of Torrens Valley Christian School's computer network, internet access facilities, computers and ALL school equipment/devices, on or off the School site, is limited to educational purposes as appropriate to the School environment. This applies whether or not the ICT equipment is owned by the user or is owned by the School. Any exception to this requirement is solely at the discretion of the School.
- 1.2. Torrens Valley Christian School has the right to monitor, access, and review all the use details in 1.1. Torrens Valley Christian School can use any means it chooses to ensure appropriate use of ICT devices and the School network. This includes personal emails sent and received on the School's computers and/or network facilities, either during or outside School hours. The School maintains the right to lock/disable/remove/modify domain/local computer accounts where deemed appropriate at its sole discretion.
- 1.3. The use of any privately or School owned ICT equipment/devices on the school site, or at any School-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 School site, or to any School-related activity. Any person unsure about whether or not it is appropriate to have a particular device at Torrens Valley Christian School or at a School-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the Torrens Valley Christian School's ICT Staff. Note that examples of a 'School-related activity' include, but are not limited to, a field trip, camp, sporting or cultural event, *wherever* its location.
- 1.4. Despite our best efforts, when using a global information system such as the internet, it may not always be possible for the School to filter or screen all material. This may include material which is **inappropriate** in the School 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.

Each and 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 School's computer network, internet access facilities, computers, and other School ICT equipment/devices. This also includes subsidiary or public organisation(s) equipment which may extend and/or be part of the School 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 (such as portable CD and DVD players), gaming devices and any other, similar, technologies as they come into use.

Users: all students that have access to Torrens Valley Christian School's ICT systems with a TVCS user name 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.

References:

www.cybersmart.gov.au

www.bullyingnoway.gov.au

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

Australian Communications and Media Authority

Related Policies:

TVCS Parent and Student ICT User Agreement

Evaluation

This procedure is to be reviewed as part of a 3 yearly review cycle.

Document Information

Document Code: Policy – Digital Citizenship

Date of issue: May 2022

Last Updated: May 2022

Author: eLearning Coordinator

Communication: Intranet

Owner: eLearning Coordinator