



Policy Title:	STUDENT ACCEPTABLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY POLICY
Policy Domain & Number:	
Effective as at:	September, 2023
Last Revised:	August, 2023
Responsibility for this Policy:	Director of Teaching & Learning
Review Date:	February 2026

1. Policy Statement

The following policy is inclusive of all Information and Communication Technologies (Hardware, Software, Communication, Actions and Data) used at the College, within College systems/licensing, as a member of the college and/or property of the college. It therefore is inclusive of personally owned devices such as laptops, tablets and mobile phones. There are unique and particular guidelines and regulations that apply to our BYOD program, these are detailed within the BYOD User Agreement.

St. Dominic's College wishes to encourage the use of Information and Communication Technology (ICT) in serving its *Learning Framework*. The purpose of the College computer network is to facilitate **educational use** of the Internet, software applications, technology and the College Intranet. This includes access to our Learning Management System, online textbook delivery, course content and resources, assessment material, feedback, grades and marks, teacher and College communication and the facilitation of collaborative and student-led learning.

Use of ICT is a requirement that comes with accountability. In order to ensure the security of the College ICT facilities and the privacy of its users, all individuals must use ICT in a responsible, efficient, ethical and legal manner. All actions undertaken by an individual's account or on their device is the direct and explicit responsibility of that individual.

2. Statement of Principles

The College has an expectation that students are responsible users who will:

- Respect the Catholic values of our College.
- Use the resources, infrastructure and Learning Management System to improve their learning and positively contribute to the learning environment.
- Knowingly view and use only what the College community considers appropriate and acceptable material.
- Never include any inappropriate ¹ material or correspondence.
- Understand that all College systems and environments are monitored and moderated by the college.
- Accept the limits the College places on the type of internet sites and security structures which may be used.
- Understand and accept that all ICT use is undertaken under the guidance and leadership of the teaching staff. Teacher leadership will modify the use of ICT in required circumstances.

¹ Inappropriate content: Content that is considered unsuitable (as per content classifications) or harmful to students. This includes but is not limited to; material that is pornographic, that promotes illegal activities, violence or prejudice on the grounds of race, religion, gender or sexual orientation.

- Recognise that for the purposes of learning, teachers may allow students to utilise personal devices in class. Failure to comply will result in disciplinary action in accordance with our *Pastoral Care and Discipline Policy*.
- Accept that all material published on the SDC network are copyrighted. Normal copyright laws apply to any sites accessed through intranet links or as a result of research for College units of work. See *Copyright Guidelines and Support*.

3. Processes

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be responsible for any breaches caused by other person(s) knowingly using their account access.

Any breach of this policy is actioned by the individual teacher, utilising the College Pastoral Care and Discipline Policies. Any ongoing concerns are referred to the relevant KLA Coordinator and may be referred onto the Pastoral Coordinators in cases that exist across more than one single faculty.

- Pastoral and Discipline Procedures
- Student Welfare and Discipline Policy
- College Bullying Policy
- Suspension and Expulsion Policy
- Procedural Fairness
- Detention Policy Statement

Device, Action and File Access

The College has the right to check all written, graphic, audio and other materials created, produced, communicated, stored or accessed by privately owned devices whilst on the College premises and/or utilising the college network and/or investigating circumstances associated with members of the College. Devices and or files may be taken and accessed if it is believed that:

- There has been or may be a breach of law; or
- there has been or may be a breach of the College rules or a College policy; or
- there may be a threat of harm to any member of the College community or system security.

If unacceptable files and/or content is found those files/content may be confiscated or deleted, and disciplinary action may be taken. If the circumstances warrant, the College may also pass the material to the police.

**Students are held responsible for
any breaches caused by them, their device and/or their College-based account.**

St Dominic's College will:

- commit to safe and responsible use of digital technologies as an integral component of the learning and teaching programs.
- provide information in relation to student access and usage of its network and reserves the right to restrict or remove student access to the facilities if students or parents do not adhere to the College usage and access guidelines.
- will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have the responsibility to incorporate these safe practices in their daily behaviour at the College.

- exercise their duty of care to students, but protection, mitigation and discontinued access to harmful information requires responsible use by the student.

Students and parents/carers should:

- understand the responsibility and behaviour requirements that come with accessing the College ICT facilities and ensure they have the skills to report and discontinue access to harmful information if presented via the internet or email.
- be aware that the ICT facilities should be utilised with good behaviour as stipulated, and students breaking these rules will be subject to appropriate action by the College.
- be aware that access to ICT facilities provides valuable learning experiences, therefore giving students educational benefits in line with the College Educational program.

Acceptable use includes:

- Following all legal and copyright regulations relating to software and intellectual property right. *Copyright Policy and Guidelines*.
- Following all College procedures and policies in relation to student welfare.
- Following all College procedures and policies in relation to our Learning Management System and *BYOD User Agreement*.
- Maintaining the security of access codes and passwords. Your device, username and password (and any action undertaken by them) are your responsibility.
- Using the network in a way that will not disrupt its use by others.
- Referencing the use of material from the internet in line with accepted practices stipulated by NESA ([All my Own Work](#)).
- The use of College communication licensed platforms (which are recorded by the College) in promoting a safe and transparent environment.
- Using all electronic devices carefully and following all teacher instructions about how and when to use them and how to take care of them.
- All users are expected to abide by all pastoral guidelines while in the online environment.
- Use of headphones that allow for learning content (video, podcast etc.) are to be used discretely and under direction of the teacher.
- Notification to their supervising teacher or parent if the student inadvertently encounters material/communication which is inappropriate or offensive (including any internet site accessed that is considered inappropriate).
- Promptly informing their supervising teacher if they suspect they have received a cybersecurity threat, computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- Ensure that personal use is kept to a minimum and internet and online communication services is generally used for genuine curriculum and educational activities. Downloads are managed and communicated per account and excessive use will result in disciplinary action by the College.

Unacceptable use includes:

- Accessing of inappropriate or offensive material (according to censorship classification, discrimination, or harassment) including games, multimedia and software applications.
- Downloading excessive amounts of data other than in the ordinary course of learning
- Installing or attempt to install software (licensed, shareware, freeware, evaluation or otherwise) on college loan devices
- Engaging in threatening behaviour, cyber bullying, making unreasonable demands, or using harassing materials or any other behaviour which is abusive or otherwise offensive.

- Deleting, modifying, stealing, and copying files or documents belonging to other users.
- Having a Virtual Private Network (VPN) installed on a student device
- Attempting to bypass, degrade or disrupt equipment, network infrastructure, and software or system performance, including the use of Virtual Private Networks (VPNs)
- Taking unsolicited photos or video of others within the College community without their consent.
- Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place at the college.
- Using technology in an act of academic malpractice (*Assessment Policies and Procedures 7-9, 10-12*).
- Use the College name or crest without the permission of the College Principal.
- Electronic communication between teachers, parents and students must only take place via COLLEGE BASED communication systems and our Learning Management System. (*Social Media and Student Communication Guidelines*).
- Not appear in College uniform or use the College Crest on any non-college authorised social network site.
- Posting (or engage in) any false or defamatory information about the College or any member of the College community.
- Using an account owned by another user.
- Using the network for any illegal activity, including violation of copyright, or other contracts and any Local, State or Federal Law.
- Vandalising the data/equipment of another user, including users within the College
- Non-educational use during class time.
- Knowingly initiate, engage with or forward communication containing:
 - a message that was sent to them in confidence.
 - a computer virus or attachment that is capable of damaging recipients' computers.
 - chain letters and hoax emails.
 - spam, e.g. unsolicited advertising material.
- Send or publish:
 - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
 - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person. As per *College Bullying Policy*. –
 - sexually explicit or sexually suggestive material or correspondence.
 - false or defamatory information about a person or organisation.
 - An unreasonably large number of emails or Canvas messages designed to inundate the recipient's inbox.
- Damage to the property of others (*Pastoral Care and Discipline Policy*)

Related Documents:

BYOD Equity Policy

BYOD Program

BYOD User Agreement