ACCEPTABLE USE OF INFORMATION TECHNOLOGY BY STUDENTS

In the spirit of right relationships, we aim to promote the integrity of all individuals within the community and develop the students as responsible and honest citizens who relish what is right and just. It is with tis common understanding that we call upon students to use technology in a way that honours the sacredness of each person as well as enhancing their own educational potential.

Information Technology encompasses all Information and Communication Technology (ICT) facilities and services provided by John Therry Catholic High School (the School), as well as equipment owned, leased, or borrowed by students. This includes, but is not limited to:

- All computers and associated ICT networks, internet access, email, hardware, data storage, computer accounts, software (both proprietary and those developed by the School) and telephony services.
- Physical spaces that incorporate ICT including teaching spaces, study areas and computer laboratories.
- ICT services provided by third parties that have been engaged by the School.
- Student owned, leased, or borrowed devised used as part of, or in conjunction with the School's Bring Your Own Device (BYOD) technology program.
- Student owned mobile phones and other devices that have the ability to access the internet; are able to record/playback audio and/or video; or can be used to transmit/receive/store/recall text, voice and/or data.
- This policy also applies to the use of these devices during school events such as excursions, camps, and extracurricular activities; and any use of social media in the context of the school community.

RESPONSIBILITY OF STUDENTS

- Students should avoid bringing non-essential forms of Information Technology to school whenever possible, except where it is a requirement for learning.
- Information Technology is only to be used in class by instruction and under direction of a staff member. Staff may grant permission for the use of particular items for a specific educational activity only. In these instances, the student is only permitted to use the item for the purpose directly specified by the classroom teacher or other staff member.
- Information Technology is not to be used between lesson times or during recess and lunch in the playground areas unless instructed by a member of staff. If a student needs to use Information Technology during recess or lunch for the purpose of education, they can do so under the supervision of staff in areas designated by the Learning Technology Coordinator.
- Students are responsible to ensure that their devices are charged and ready for use each day.
- All items of Information Technology not used for learning must be switched off to ensure that lessons are not disrupted.
- It is the student's responsibility to ensure the safekeeping of their Information Technology.

- Students should not be involved in the unauthorised use, tampering, theft or intentional damage of another student's Information Technology.
- During examinations all items of Information Technology must be handed in to the Examination Supervisor before the commencement of the examination. This will be returned to the student at the completion of the examination.
- In the case of a lockdown or fire emergency, students are not permitted to use an Information Technology Device. In these instances, all devices must be turned off, even if the emergency occurs outside of school hours.

PRIVACY AND CYBERBULLYING

- It is prohibited to use cameras, photographic, or audio recording devices without the permission of both:
    - a staff member and
    - the person being filmed, photographed or recorded.
- Items of Information Technology are not to be used or taken into changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.
- Students are responsible for the security, privacy and confidentiality of data of a private or personal nature, held or transmitted using Information Technology.
- Any attempt (successful or otherwise) to invade the privacy of others using ICT resources will be regarded as a breach of this policy.
- Passwords and login details are provided for the sole use of the authorised user. They should be treated as private and confidential, and must not be divulged or distributed.
- Users must use only their own credentials on School Information Technology resources. Users are not permitted to access or attempt to access any program, file or other information stored under another person's account.
- Users must not attempt to obtain credentials they are not entitled to know. This is applicable to accounts or facilities on School computers or other computers accessed using the School network.
- All School owned Information Technology resource usage is logged and may be audited. Use of resources may be logged and audited by participating organisations. Usage and activity records belong to the School, not the individual user. In most cases, these are admissible as evidence and are subject to relevant State and Federal Laws.

THEFT AND DAMAGE

- The school accepts no responsibility for Information Technology items if they are lost, misplaced or damaged while on school premises.
- The school accepts no responsibility for students who lose or have their items of Information Technology damaged or stolen while travelling to and from school.
- Students who bring items of Information Technology to school should:
    - mark their item with their name
    - not leave the item unattended or out of sight unless under instruction
    - not allow other students to use the item
- Items of Information Technology found in the school should be handed to the front office staff.

CONTENT AND COPYRIGHT

- Information Technology must not be used for preparing, storing, receiving, displaying, transmitting or communicating information, material or messages:
    - that are inconsistent with the mission or Catholic values of the School
    - that may have the effect of harassment of any person, or
    - that may be defamatory
    - this includes but is not limited to pornography, racism, sexism, obscenities, insults, threats or intimidation
- Students are not to send inappropriate material of themselves or others, and should never request that other students send inappropriate material to them. This is a criminal offence, and the School has an obligation to report these to the relevant external law enforcement agencies.
- If a student receives an inappropriate image or film via their Information Technology they must immediately inform a staff member. Under no circumstances should the student forward this onto another person. In these instances, persons who forward on images will be held equally responsible as the person who originally captured and sent the images. This is a criminal offence and the School has an obligation to report these to the relevant external law enforcement agencies.
- Risks to students that involve use of the Information Technology can generally be considered foreseeable risks of harm or injury, which the School have a duty of care to take steps to prevent. Web filtering is one method used to ensure a safe environment for students and any attempt (successful or unsuccessful) to circumvent School web filtering is considered a serious breach of this policy.
- Information Technology resources are not to be used to gain unauthorised access to other computers/networks/systems/files/data, regardless of the intention.

- Users must not install or use unlicensed or malicious software on School or student owned, borrowed, or leased Information Technology, nor circumvent the School's IT security measures.
- The School supports and encourages the legitimate use of digital media to enhance the teaching, learning and research activities of the School. However, the School does not condone any activity which infringes the rights of any third party. All students are responsible for observing copyright legislation, and any restrictions or obligations under any licences or permissions in their use of digital media.

MOBILE PHONES AT SCHOOL

- John Therry Catholic High School accepts that parents/guardians/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. It is acknowledged that providing a child with a mobile phone gives parents/guardians/carers reassurance that they can contact their child if they need to speak to them urgently, while their child is travelling to and from school.
- If a student needs to use a mobile phone during the school day for extenuating personal circumstances, they must come to the front office where they will be granted permission to turn on the phone and use it in a supervised location. When they leave the office the phone must be switched off. Parents should expect that the student will receive the message on their mobile phone after the final bell at the end of the school day and are, therefore, permitted to switch it on.

CONFISCATIONS

- Where a student has breached this Policy, or where there is reasonable suspicion that a student is in breach of the policy, the School reserves the right to confiscate items of Information Technology for the remainder of the lesson, or while the matter is investigated.
- Students must comply with a request by a member of staff to surrender item(s) of Information Technology. Failure to comply may constitute misconduct under other School policies as deemed appropriate by the School Principal.
- Information Technology items are confiscated until the end of a lesson, except where a breach of policy involves privacy concerns, risk to safety, or unethical/illegal activities, where it will be held until further investigation by the School or relevant external law enforcement agencies.
- Two (2) confiscations in the period of a school year will require students to complete a Smart Use of Technology program during a lunch or recess detention scheduled by the Learning Technology Coordinator.
- Three (3) confiscations in the period of a school year will require students to complete a Smart Use of Technology program during an afternoon detention scheduled by the Learning Technology Coordinator.

- Multiple confiscations in the period of a school year will result in further consequences, and may constitute misconduct under other School policies as deemed appropriate by the School Principal.

BREACH OF POLICY

- Breach of this Policy will be judged on a case-by-case basis and if judged to be serious, will result in further consequences and may constitute misconduct under other School policies as deemed appropriate by the School Principal.
- Repeated infringements may result in suspension of access to specific School ICT resources and the withdrawal of the agreement to allow the student to use Information Technology at the School.
- The School may take any action deemed necessary to remedy immediate threats to School ICT resources including, without limitation, suspension of access, confiscation of Information Technology and/or disconnecting or disabling equipment with or without prior notice.
- Where a breach involves unethical or illegal activities, the School has an obligation to report these to the relevant external law enforcement agencies, and individuals may be subject to prosecution.
- Breach of this Policy will result in a detailed entry on the student's permanent record.
- The School will notify parents/guardians/caregivers of any breach by the issuing of a red stamp in the student's School Planner; or by phone, email or letter where breaches are deemed to be more serious.

AGREEMENT

The terms and recommended conduct described in this agreement are not intended to be exhaustive, nor do they anticipate every possible use of the School's facilities. You are encouraged to act with caution and take into account the underlying principles intended by this agreement. If you feel unsure of the appropriate action relating to use of Information Technology, you should contact the Learning Technology Officer, School Technology Officer or School Principal.

It is the responsibility of students who use Information Technology at school to abide by the guidelines outlined in this document.

It is the responsibility of the parent/guardian/carer to monitor the content of the student's Information Technology to ensure that it adheres to the guidelines outlined in this policy.

Permission to use Information Technology at school while under the school's supervision is contingent on parent/guardian/carers permission in the form of a signed copy of this policy.