ST TERESA'S CATHOLIC COLLEGE

# ICT and Device Policy, Guidelines and Use Agreement



Brisbane Catholic Education
teaching • challenging • transforming

45 Sea Eagle Drive, Noosaville Qld 4566 | www.stteresa.qld.edu.au

# Table of Contents


**Introduction** ..... 3

**Rationale** ..... 3

**Important terms used in this document** ..... 3

**Principles** ..... 3

*Ownership* ..... 3
*Cyber-safety* ..... 3
*Acceptable Use* ..... 4
*Internet Access* ..... 4
*Technical Issues* ..... 4
*Passwords* ..... 4
*Lost/Unattended Devices and Accessories* ..... 4
*Replacement Devices* ..... 4
*Students taking their Devices on Holidays* ..... 4
*Care of Devices* ..... 5
Storage ..... 5
Handling ..... 5
*Cleaning* ..... 5
Screen ..... 5
Case/Cover ..... 5
Keyboard ..... 5
*Charging* ..... 5
*Installation of Programs* ..... 6
*Email* ..... 6
*Saving of Items* ..... 6
*Warranty and Non-Warranty* ..... 6
*Insurance* ..... 6
*Theft, Loss or Damage of Accessories (Chargers, Protectors)* ..... 7
*Termination Agreement* ..... 7

**Acceptable use of Devices and Digital Resource** ..... 7

*Responsibilities of Users* ..... 7
Permitted use of technology resources ..... 7
Confidentiality and Cybersafety ..... 8
Cyberbullying and defamation ..... 8
Security ..... 8
Copyright ..... 8
Consequences following a breach of this Acceptable Use Statement ..... 8

# Introduction

The College's computer network, Internet access facilities, computers and other College ICT equipment/devices bring great benefits to the teaching and learning programs at St Teresa's Catholic College, and to the effective operation of the College. This applies whether the ICT equipment is owned or leased either partially or wholly by the College and used on or off the College site.

The devices issued to students in the College are viewed as another tool used in the classroom. They allow students to approach their learning in a different fashion and to explore concepts and ideas more broadly than previously possible. They are not, and never will be, the primary focus of the classroom.

# Rationale

This document outlines the responsibility of the parties involved for the provision and use of the 1:1 Device Program at the College. It clarifies the ownership of the devices, the provision of the devices and related services and the responsibility of the parents and students for the use and care of the devices.

# Important terms used in this document

- The abbreviation 'ICT' in this document refers to the term 'Information and Communication Technologies'.
- 'Information Technology' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.
- 'College ICT' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined below.
- The term 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, iPads, PDAs), storage devices (such as USB and flash memory devices, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players and any other, similar, technologies as they come into use.
- 'Objectionable' in this document means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment.
- The term 'parent' used throughout this document also refers to legal guardians and caregivers.

# Principles

## Ownership

Ownership and control of the device, its accessories and software always remain with the College. The parties acknowledge the student will have day to day possession of the device whilst they are enrolled at the College. The College always reserves the right to:

- Decide who uses the device and the use to which device is put; and
- Recall the device for any reason (including upgrading firmware, inspecting it to check its operational performance and ensuring that the device is used only as provided under this policy.

Devices are issued in 3-year cycles, with Year 7-9 students using an iPad and Years 10-12 students using a laptop. Year 9 students must return their iPads and accessories at the end of Year 9 in order to receive a laptop for the remainder of their schooling at St Teresa's.

## Cyber-safety

All students in the College will undergo training in the various aspects of cyber-safety throughout their time at the College. Topics covered will be relevant to the particular year level and issues currently of concern.

## Acceptable Use

- Students will use their device during class time as and when instructed by the classroom teacher.
- Screens must be partially or fully closed when the teacher is addressing the class.
- Installation of inappropriate programs or visits to inappropriate websites may result in the loss of device access for the student for a prescribed period of time.
- Students must prioritise educational use of their device over personal use. This includes but is not limited to: applications; documents; movies; music and photos.

## Internet Access

- Internet access during school hours is provided by the College.
- Internet usage is monitored by College Staff and filters put in place by the College will apply.
- Students can connect to the internet at home via wireless access if available and approved by parents.

## Technical Issues

- The College employs IT Technicians to provide assistance with technical issues, repairs, loss and damage of the devices during term time. No repair, service or other work is to be carried out by an external party at any time.
- Students will report any technical issues to the IT Technician as soon as possible after they become aware of the issue.

## Passwords

- Students must select a secure password and keep their username and password information private. The password should be changed regularly.
- Should the password for the portal be forgotten, students are to contact a College IT Technician, the password will then be reset.

## Lost/Unattended Devices and Accessories

- Devices are not to be left unattended at any time.
- If devices are found around the grounds or sitting on lockers, they will be removed and taken to Student Administration or the House Group Leader.
- Students will need to collect and sign for the lost/unattended device.
- Repeat offenders will incur appropriate consequences from the Pastoral Leaders.
- If a student loses their device, it is to be immediately reported to the College IT Technician or House Group Leader.
- If, after a reasonable period of time, it has not been located, an insurance claim will be processed.
- If a student loses or damages their charger is the student or caregivers' responsibility to replace the charger with a genuine apple charger or reputable equivalent.

## Replacement Devices

- There will be a limited pool of spare devices that may be loaned to students whilst theirs is repaired.
- Spare devices may not be loaned out in cases of deliberate damage or damage caused by user carelessness if the College is short of spare devices.

## Students taking their Devices on Holidays

It is realised that the likelihood of damage/loss while on holidays in Sydney, or Melbourne or even overseas would not be much different from that which could occur going to Brisbane for the weekend.

Devices can be taken on holidays but travel to particular places will bring different risks, therefore every effort should be made to minimise these risks. There is no need to inform the College of such travel, but the College will need to be informed if there is loss or damage.

Be aware that families won't be able to recoup any costs through travel insurance. An insurer would ask for evidence of ownership which of course parents won't be able to produce, as the device belongs to the school.

## Care of Devices

### Storage

Both formative and summative assessment may occur during scheduled subject class time as specified in the assessment calendar. For the junior school there may also be designated times at the end of each term for longer examinations or where there are multiple classes for the same subject.

- Devices are to be stored safely and securely when not in use and when being transported between classes, and to and from school.
- The identity sticker and protective cover supplied by the College must remain on the device and not be removed unless by the IT Technical staff. Failure to follow this rule may result in insurance becoming void if the device is damaged from being knocked or dropped accidentally without the protection of the case.
- Stickers, graphics, drawings and other markings must not be placed anywhere on the device, including on the cover.
- During school hours, when the device is not required, it is to be stored in a locked locker.
- Under no circumstances are devices to be left in lockers overnight. To do so will void insurance cover.

### Handling

- Devices are to be used on a stable surface such as a desk, not on laps.
- Devices are not to be carried with their lids open.
- It is important to check there is no pencil, earphones, etc on the device keyboard before closing the lid or protective cover.
- Laptops are not to be lifted by the screen as this will cause damage the hinges and display over time. Such damage is not deemed to be accidental.
- Devices are not to be used whilst drinking – spilt liquid can be fatal to iPads and computers!
- Device keys are to be kept intact and not picked at – charge will be incurred to repair keys if damaged.

## Cleaning

### Screen

- Dampen a soft, lint-free cloth with water only, then use it to clean the computer's screen.
- Avoid applying pressure to the screen.

### Case/Cover

- Clean with a soft, damp cloth.

### Keyboard

- Gently brush with clean, soft-bristled brush or use the same method as for the screen.

## Charging

- It is the responsibility of the student to arrive at school each day with their device fully charged.
- When charging is necessary and available, a student will be moved to locations near power points in the classroom. It is preferrable that chargers remain at home for charging of devices overnight, so they are not lost/misplaced.

- Students log in to their device at the start of the day, then simply shut the lid or cover between lessons. This will put the device into hibernation mode and simply requires unlocking using their password to “wake up”.

## Installation of Programs

- Devices will initially be imaged with the minimal programs required at the College (a “thin” image).
- Additional programs can be installed via the application Self Service
- Students are not permitted to delete any programs installed by the College.
- Further programs/textbooks required for class will be installed by students as necessary.
- Students can download/install programs of their choice providing they have legal ownership of, or entitlement to, the program.
- Students are not permitted to download games or game launchers on their device.

## Email

- The majority of communication from the College to students will be done via their Brisbane Catholic Education emails (username@mybce.catholic.edu.au).
- Students are expected to check this email daily.
- Students are not permitted to use their school email account for personal usage such as: signing up to newsletters, streaming services, buy/sell sites, chatroom for messaging friends or other students.

## Saving of Items

- Students have access to OneDrive and Microsoft365 accounts (attached to their email accounts).
- Students are encouraged to store documents in one of these and to regularly back up documents to a separate storage device as security.
- Students are discouraged from using their device hard drives as a sole storage point for documents, as the data may be lost during reimaging or repair of the device.
- College IT Technicians will not retrieve data stored on device hard drives.

## Warranty and Non-Warranty

All warranty claims will be assessed by an authorised repairer. In cases where the repairer determines that the repair does not meet the warranty conditions, an insurance claim may be made through the College.

- The devices and batteries are covered by a 3-year warranty.

## Insurance

Should an insurance claim be made in respect of the device and be accepted by the insurer, the charge to the parent is as stated below:

- An excess of $150 will be payable for each claim.
- In cases where damage/loss/theft is incurred to the device and two claims have previously been made in one year, the full cost of repairs or replacement will be paid by the parent.

The insurer will exclude a claim in particular circumstances. These may include:

- Wilful damage of device.
- Theft or damage while left unattended and out of view of the student. This includes leaving the device in unlocked locker, outside a shop, on a school sport field, school bus shelter, unattended on top of a locker, or unattended in a classroom outside of normal school hours.
- Theft from an unlocked locker.
- Scratching of the casing and/or bruising/cracking of the screen because of misuse.
- Damage to device because of protective cover removal.

- Damage to protective cover through misuse.
- Theft or loss of the ac adaptor or power cords.
- Theft of device left on college premises overnight, during weekends or school holiday periods.
- If damage is caused to another student's device due to another student's misuse, the insurer will exclude the claim. The parent will be required to meet the College's cost of the repair work or replacement where appropriate. The repair costs (parts and labour) or replacement cost will be charged to the parent.

## Theft, Loss or Damage of Accessories (Chargers, Protectors)

A fee will apply to replace the Device Charger, and Protective Cover for any loss, theft or damage to these items. You are not able to purchase these items externally as they remain part of our device package and must meet warranty and Workplace Health & Safety requirements.

## Termination Agreement

This agreement terminates when the student leaves the College at the end of his/her enrolment or when the College otherwise requests the return of the device. The student must return to the College:

- upon receiving a request from the College to return the Device; or
- at the end of the student's enrolment and prior to the student leaving the College.

It must be ensured that the device and charger are in good working condition when returned to the College or cost of damage will be charged.

If a student fails to return the device and accessories when they leave, the College will undertake action to retrieve them. Any legal or other costs associated with the retrieval are at parents' expense.

# Acceptable use of Devices and Digital Resource

Devices and digital resources have become of critical importance to schools in facilitating and supporting learning and teaching. **Technology resources are provided to students for educational purposes only.**

**St Teresa's Catholic College** has established significant digital resources to support these activities. This includes technology provided on College grounds and College owned technology that may be taken off the College grounds with permission from the College. **St Teresa's Catholic College** has specific guidelines relating to the use of technology **[ICT and Device Policy, Guidelines and Use Agreement]**

This document has been developed to inform users of their rights and responsibilities when using devices and digital resources, consistent with Brisbane Catholic Education's requirements that all such resources are used in an ethical, legal and responsible manner.

The requirements and rules set out below apply to all **St Teresa's Catholic College** technology resources whether they are accessed through devices owned by the College or through privately owned devices.

Please read this document carefully. Each student and his/her Parent/Legal Guardian must sign the acknowledgment to confirm that they understand the requirements of acceptable use and the potential consequences of a breach of this document.

## Responsibilities of Users

### Permitted use of technology resources

1. Students must only access **St Teresa's Catholic College** technology resources for schoolwork. **Students must not:**
    a. buy or sell items or services over the internet.
    b. access or enter online communication outside of school authorised platforms.
    c. access, post or send inappropriate digital content. This includes but is not limited to; content that is illegal, dangerous, obscene, offensive or could be considered bullying or harassment.
    d. amend documents created by another person without the author's consent.

e. download, install or use unauthorised computer applications.
f. deliberately install viruses or other malware.
g. gain unauthorised access to any system or information by any means.
h. use technology to attack or compromise another system or network.

## Confidentiality and Cybersafety

2. Students should be aware that material they post online (including-social media sites) is **public**. The content of public posts may have personal implications for students if, for example, potential employers access that material. The content of posts also reflects on our educational institution and community. Once information is on the internet it may not be possible to remove it. Students must be aware of their digital footprint and the lasting impact that it can have to their lives and that of others.
3. For the safety of students, personal information about themselves or others should not be published publicly. For example, students should not post their own or anyone else's address, telephone number or other personal details online. Students should not distribute someone else's personal information without informed consent from the individual or their guardian.
4. Students should be aware that persons on the internet might not be who they say they are. Students must not arrange to meet persons who they have met online.
5. **St Teresa's Catholic College** may also be required to inspect or provide copies of electronic communications where required to by law, or where the investigation of possible misuses of technology resources is required.
6. Students should be aware that 'Cloud' based tools and services are used for data storage and learning opportunities. Some of these services may store data on servers located outside Australia.

## Cyberbullying and defamation

7. Students are prohibited from using digital or online tools to communicate or publish derogatory, impolite, or unkind remarks about others, or to send threatening, harassing, or offensive messages. Improper use of digital platforms and resources may result in defamation and be referred to legal authorities.

## Security

8. Students must regularly check for and complete updates on their devices to ensure they remain secure.
9. Students must use a secure password or passphrase and keep their username and password information private. The password should be changed regularly in line with the Australian Curriculum and should be difficult for other people to guess. Students should take steps to ensure their device is inaccessible to others when unattended, e.g., lock screen.
10. Students must not use another person's name and password to access resources.
11. Students must report a suspected breach of security to the College.

## Copyright

12. The use of material from the internet may be a breach of copyright or other intellectual property rights. Students must not use **St Teresa's Catholic College** technology resources to copy, download, store or transmit any such material that may include music, images, videos or any other form of media.

## Consequences following a breach of this Acceptable Use Statement

1. A breach of this statement will be taken seriously and may result in disciplinary action.
2. Any known breaches of these Acceptable Use conditions must be reported by **St Teresa's Catholic College** to Brisbane Catholic Education's Legal Counsel and/or Head of IT.
3. Examples of possible consequences range from **St Teresa's Catholic College's** ICT and Device Policy, Guidelines and Use Agreement.
4. Students and Parents/Legal Guardians may be financially liable for damage caused to resources.
5. Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.