WAVERLEY COLLEGE

Responsible Use of Technology Policy

Introduction and Definition

This policy relates to the use of Technology by students where the primary use is for student learning. This includes school owned and issued laptops, iPads and any other technology related resources.

This policy also extends to the appropriate use of storage locations whether that is physical USB storage or cloud locations.

This Policy also includes the rules around acceptable use of technology (Section 2 below)

The policy does not relate to student mobile phones as this is covered in the Mobile Phones policy which can be found in the Student Diary.

Usage of Technology when in school

The following general rules apply to the use of technology when at school.

- Technology should be used for positive purposes: for learning, for legitimate communication or research.
- During class and study time, the internet may only be accessed through the College network - Students may not access the internet through another account or means.
- Students are expected to comply with the standards and act within the ethical framework of this Catholic College, where respect for individuals, their good name and dignity is paramount.
- In some situations, such as formal Examinations, other specific rules may apply to Technology, such as online NAPLAN etc. These will be outlined clearly at the time and must be adhered to fully.
- Any inappropriate use of the College name or resources in any form is totally unacceptable. This includes but is not limited to the posting of inappropriate material or comments relating to members of the Waverley College community onto Social Media platforms.
- Technology should not be used to harass or victimise other students or staff, or abuse a person's right to privacy (for example, taking, storing and then using a digital photo/video without a person's permission).
- A staff member who has reasonable grounds to suspect that Technology is being, or has been used inappropriately can request access to the device or escalate this to the College iAssist Team to investigate.

EDMUND RICE EDUCATION AUSTRALIA

WAVERLEY COLLEGE

Consequences

Students who breach any of the regulations contained in this Policy will receive a Saturday Detention in the first instance. More serious breaches of this policy will result in suspension and enrolment review.

Section 1 - Detailed information

Security of Technology

It is the responsibility of students to ensure that technology, either personal items or school issues items are secured in an appropriate way.

- Students are responsible for the security and condition of any technology issued to them.
- The College takes no responsibility for damage or theft of a student's Technology when brought onto Campus.
- Students should lock your personal Technology in their locker during the course of the school day when not in use.
- Do not leave items of Technology in items of clothing that you are likely to remove – e.g., blazers
- Do not leave items of Technology in school bags if those bags are unattended.
- Do not bring items of Technology in on special activity days – such as sports days, swimming carnivals, athletics championships, etc. Unless pre-approved by an appropriate member of staff.
- Students should not bring laptops that are not part of the College Laptop Program onto College premises. This includes end of lease devices that have been purchased from prior years.

WAVERLEY COLLEGE

Use of Technology during school activities

For certain activities and excursions students may be permitted to take along items of Technology. The following rules apply.

- The teacher or supervisor in charge of any activity such as excursions, camps, retreats etc will advise whether students can bring along items of technology.
- If Technology is permitted, it remains the responsibility of the student to ensure that it is secured, maintained and used appropriately.

Rules specific to School Issued Laptops

All students are issued a fully managed laptop for use for Educational purposes only. Waverley College has the ability to remote into laptops without warning to ensure the safe use of these units whilst in school.

- Devices are issued for school use only and software is installed and managed centrally by the iAssist Team.
- Games and unlicensed software should not be installed / run on these devices.
- These devices should not be used for hacking, cracking or any other illegal activities.
- Students are responsible for the device that is issued to them, they should ensure that it is kept in working order and report any faults and damage to iAssist as soon as it is discovered.
- There is no charging in school, this means chargers issued at deployment are to remain at home. Laptops should be brought to school fully charged each day.
- Laptops are issued with covers and these should remain on the device.
- Whilst in school students should not tether their laptops to mobile devices.

- Laptops are fully managed and will be shutdown in accordance with current policies as follows, students should not attempt to circumnavigate these times.
    - Year 5 and 6 - Shutdown between 9pm - 6am
    - Year 7 to 9 - Shutdown between 10.30pm - 5am
    - Year 10 to 11 - Shutdown between 12am - 5am
    - Year 12 - No shutdown

Rules specific to USB storage devices

In the first instance students should use their school managed Google Drive when sharing educational relation material with their peers (see section below).

- Students are allowed to use USB storage devices for transferring school-related data to and from the College.
- When brought on campus USB drives are to be free from files that contain inappropriate, offensive or illegally obtained content.
- A Staff member may inspect a USB drive at any time if they suspect a breach of this policy. Students found with offensive, inappropriate or non-educational material will be referred to their Head of House.
- If students bring USB storage devices into school they are responsible for securing and managing the device, the school takes no responsibility if the device is lost, stolen or damaged.

Rules specific to cloud storage locations

- School managed cloud storage locations include Google Drive and should be used for sharing and storing educational material.
- Students should use Google Drive to backup any critical school files this will allow iAssist to restore them in the event of an issue with their laptop.
- Cloud storage should not be used to store inappropriate content such as games, images, video etc
- Sharing of content from Google Drive should only be carried out for school purposes.

- Students will not be able to share content with external, non-Waverley accounts.

- Should there be any suspected breach of the use of Google Drive, iAssist will be able to access and check the content once approved by the Director of ICT.

Section 2 - AUP

Acceptable Use of IT (AUP)

All students at Waverley College have access to the college network. Waverley College embraces emerging digital technologies and encourages its teachers and students to look for ways of using them to enhance teaching and learning.

A breach of the Acceptable Use of IT whilst at Waverley is defined as:

- Any student who posts material on a website that College authorities deem inappropriate or damaging to the good name of the College will face disciplinary action. This may include immediate suspension or even exclusion from the school.

- Accessing, downloading, storing or printing files or messages that are sexually explicit, obscene, or that offends or tends to degrade others.

- Deliberately entering, or remaining in websites containing objectionable or offensive material.

- Attempting to degrade, disrupt system performance, perform processes that can result in the loss of data or attempt unauthorised entry to College systems.

- Removing, damaging or vandalising any IT equipment or interfering with any cabling connected to devices.

- Attempting to run any programs other than those sanctioned by the school on school issued devices. Including games, browser plugins or unlicensed software.

- Copying materials in violation of current copyright law or sharing such content with other students.

- Tethering school laptops to alternative mobile devices in an attempt to circumvent the schools filtering policies. Or using software to mask or operate anonymously on the school network such as VPNs.

WAVERLEY COLLEGE

Controls that are in place to monitor the network

Students should be aware that iAssist maintains a set of tools to help manage the school network and ensure it is being used appropriately by all College users. This means at any time iAssist has the ability to scan and check information being transported across the network and monitor processes and applications that are being used. If content is deemed inappropriate iAssist are permitted to block the device and escalate to the Director of ICT.

Controls include:

- All internet content is monitored and filtered whilst a student is on campus according to a predefined set of rules by the school firewall.
- All emails sent are scanned for content and messages archived.
- Next Generation Antivirus is used to protect users and will actively block unwanted, potentially malicious programs.

This policy will be reviewed inline with current procedures and the College has the right to modify any of these rules according to current circumstances and threats.

WAVERLEY COLLEGE

Section 3 - Sign Off

A copy will be held on the student's file.

We accept and agree to abide by the rules and guidelines contained within this document.

Parent Signature: _____ Date: ____/____/____

Parent Name: _____

Student's Signature: _____Date: ____/____/____

Student's Name: _____

EDMUND RICE EDUCATION AUSTRALIA