

RESPONSIBLE USE OF TECHNOLOGY

Introduction and Definition

This policy relates to the use of Technology by students at Waverley College. This includes school-owned and issued laptops, iPads, mobile phones, smart watches, headphones 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).

Usage of Technology when in School

The College wishes to maintain a balance between utilising technology to assist with learning, whilst being cognisant that students should not be connected to technology at all times. The wellbeing of students will be maintained via educational programs. 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 on 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 confiscate the device for investigation by a member of the College Leadership Team or iAssist Team.

SECTION 1 - DETAILED INFORMATION

Security of Technology

It is the responsibility of students to ensure that technology, either personal items or school-issued items are secured in an appropriate way. Students are responsible for the security and condition of any technology issued to them by the school.

- The College takes no responsibility for damage or theft of a student's Technology when brought onto Campus.
- Students should lock any 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.
- Students should ensure that passwords used to access school systems are of a complex nature and are not shared with other students or family members.

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.

- Laptops are not permitted for use in the playground or outdoor spaces between 8:15am - 3:15pm. Unless otherwise approved by the classroom teacher for specific tasks.

- Students may use their laptop within the Library for College use only (Homework or Assessments).
- Devices are issued for school use only and software is installed and managed centrally by the iAssist Team.
- Games and unlicensed software and/or browser extensions and plugins should not be installed/run on these devices.
- The use of Ai tools should be limited to platforms that have been pre-approved by the school..
- 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.
- For years 7 to 12 there is no charging facility in school. This means chargers issued at deployment are to remain at home and students are expected to bring devices to school fully charged.
- For year 5 and 6 devices will primarily remain on Campus and will be charged overnight.
- 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 shut down in accordance with current policies as follows, students should not attempt to circumnavigate these times.
 - Years 5 and 6 - Shutdown between 9pm - 7am*
 - Years 7 to 9 - Shutdown between 10.30pm - 5am
 - Years 10 to 11 - Shutdown between Midnight - 5am
 - Year 12 - No shutdown

* When laptops are approved to go home with students

Rules specific to Mobile Phones and Smart Watches

Years 5-6

Mobile phones and smart watches are not permitted for use on College grounds between 8:15am and 3:00pm. They need to be turned off and handed to the class teacher at the beginning of the day.

Mobile phones and smart watches are brought to the College at the owner's own risk. No liability will be accepted by the College in the event of loss, theft or damage of the phone.

If a parent/carer does need to contact their son, they should do so by calling the front office on 02 9387 5022.

Consequences Specific to Mobile Phones and Smart Watches (Years 5 - 6)

If a student has a mobile phone or smart watch on school grounds between the hours of 8:15am - 3:00pm, they will receive a one-hour lunchtime detention in the first instance and an afternoon detention in the second instance. In a third instance they will be suspended from school where a meeting with the Director of the Junior School will take place upon their return.

Years 7-12

Mobile phones are not permitted for use on College grounds between 8:15am and 3:15pm. They need to be turned off and placed in the student's locker within these times.

- Smart Watches are permitted to be worn but should be switched to aeroplane mode and are not to be used for communication purposes.
- Students are NOT permitted to access social media, games, texts, phone calls, cameras or applications.
- Mobile phones are not permitted for use in the playground or outdoor spaces during the above times.
- Mobile phones are brought to the College at the owner's own risk. No liability will be accepted by the College in the event of loss, theft or damage of the phone.
- If a student has exceptional circumstances that require the use of their mobile phone during College hours (such as issues relating to health or family), the Head of House should be informed and requests for exceptions made.
- If a parent/carer does need to contact their son, they should do so by calling the front office on 02 9369 0600.

Consequences Specific to Mobile Phones (Years 7 -12)

If a student has a mobile phone on school grounds between the hours of 8:15am - 3:15pm, they will receive a one-hour detention in the first instance, and a three-hour detention in the second instance. In a third instance they will be suspended from school where a meeting with the Deputy Principal-Students will take place upon their return.

If a teacher believes a student has been recording video or taking photos, their phone will be confiscated and given to the Deputy Principal-Students for further investigation.

Rules specific to Headphones

- Headphones are not permitted for use on College grounds between 8:15am and 3:15pm, unless granted explicit permission by a teacher.
- Headphones may be used for teaching and learning purposes at the discretion of the classroom teacher.
- Students in Years 7 to 12 are responsible for providing their own headphones for listening to content on their laptop.
- Headphones will be provided to students in Year 5 and Year 6 as part of their stationery pack. If any subsequent headphones are required as a result of loss or damage, this is the responsibility of the student.

Rules Specific to USB Storage Devices

In the first instance, students should use their school-managed Google Drive when sharing educational related 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 back up 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:

- Posting content to an online platform that is deemed inappropriate or damaging to an individual or Waverley College.
- Accessing, downloading, storing or printing files or messages that are sexually explicit, obscene, or that offend or degrade others.
- Deliberately entering or remaining in websites containing objectionable or offensive material.
- Attempting to disrupt system performance or 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. These include 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 school's filtering policies or using software to mask or operate anonymously on the school network such as VPNs.

Consequences for Breaching the AUP

Consequences will vary depending on the severity of the breach, they may include:

- ❖ Detention
- ❖ Suspension
- ❖ Expulsion

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 and safely 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 in line with current procedures and the College has the right to modify any of these rules according to current circumstances and threats.