Blackheath & Thornburgh College

INFORMATION, COMMUNICATION & TECHNOLOGY POLICY

Review Procedure
The Board and Principal will review the policy as required. The review schedule is directed in response to organisational and/or legislative changes and requirements. The review will be undertaken in consultation with employees and other relevant parties. All relevant persons will be made aware of changes made because of the review.

This policy will be reviewed if:

- There are changes in the workplace that may affect the policy;
- The policy is not effective;
- There are legislative changes that affect the policy; or
- There is a breach of this policy.

This policy is reviewed at least annually.

Document Number:	HR33_01a
Topic:	Information, Communication and Technology
Approval Authority:	Board of Directors
Document Owner:	Blackheath & Thornburgh College
Last Approval Date:	May 2026
Review Date:	April 2027
Audience:	All employees, students, volunteers, contractors, visitors, parents and Board members
Related Policies	Staff Code of Conduct Student Code of Conduct Student Anti-Bullying & Harassment Policy Social Media Policy Privacy Policy Data Breach Response Plan Email Usage Policy Generative Artificial Intelligence (AI) Policy
Document Web Links:	https://ppr.qed.qld.gov.au/category/technology-and-information-management https://esafety.gov.au

Purpose
Information technology (IT) is playing an increasing role in our society. It is one of the fundamentals of education and to be personally fulfilled and effective members of our community, students emerging from our College must have both competence and confidence with information technology.

Therefore, students must be afforded the opportunity to utilise information technology to enhance their own learning and to contribute to the learning of others by using information technology effectively.

Artificial intelligence (AI) is a novel aspect of using information technology and is outside the scope of this policy. Please refer to the College AI Policy for further details on this matter.

Responsibility
Principal and Risk & Compliance Officer.

Principles
Correct use of information technology contributes to the attainment of self-fulfilment, the improvement of teaching and learning.

The staff and students at the College shall have adequate access to current technology within the College's budget. The College shall provide resources to ensure that:

- There is competence and confidence in the use of information technology
- Budgetary considerations are adequate to allow access to information technology
- Systems of information technology are developed collaboratively within the College community

Based on the principles in this document, the College will continue to integrate IT across the curriculum.

Expected Outcomes
This policy aims to ensure that:

- Students will leave the College competent and confident with information technology and be able to use it to contribute to society
- Staff and student's personal growth will be enhanced using information technology
- The College will endeavour to share technological ideas, knowledge and materials with families and the external community

General Guidelines
All users should adhere to the following broad guidelines:

- Use of computer/internet resources for educational purposes has priority over recreational uses
- Appropriate language must be used in all communications including email messages, chat and web pages
- No user should deliberately or carelessly waste computer resources (e.g. unnecessary printing) or disadvantage other users (e.g. by monopolising equipment, network traffic etc)
- Consideration must be given to avoiding inconvenience to other computer users e.g. use headphones to listen to sound or music; leave computers ready for the next user to log in; not leave programs running on computers when you leave; not leave rubbish or paper lying around computers; replace furniture to normal positions when you leave

While on the College network, users should not breach the College's policies (which includes the Student Anti-Bullying & Harassment Policy addressing cyber bullying, Email Usage Policy and AI Policy).

Staff and student's use of internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Passwords
Use of the College's Information, Communication and Technology (ICT) network is secured with a username and password. The password must be difficult enough so as not to be guessed by other users and is to be kept private by the user and not divulged to other individuals (e.g. a user should not share their username and password with fellow users).

The password should be changed regularly, as well as when prompted by the College or when known by another user.

Personal accounts are not to be shared. Users should not allow others to use their personal account for any reason.

Users should log off at the end of each session and lock their computer while away from it, to ensure no one else can use their account or device.

Where a student has a BYO device, it is recommended that the student set a password for access to their BYO device and keep it private.

Parents/caregivers may also choose to maintain a password on a personally owned device for access to the device in the event their student forgets their password or if access is required for technical support. Some devices may support the use of parental controls with such use being the responsibility of the parent/caregivers.

Data and Security Back-ups
While at College, users can save data to the College's network, which is safeguarded by a scheduled backup solution.

Users are also able to save data locally to their device for use away from the College network. The backup of this data is the responsibility of the user and should be backed-up on an external device, such as an external hard drive or USB drive.

Users should also be aware that, if any repairs need to be carried out, the service agents may not guarantee the security or retention of the data. For example, the contents of the device may be deleted, and the storage media reformatted.

Privacy and Confidentiality
Users should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the College. It is important that users do not publish or disclose the email address of a staff member or student without that person's explicit permission. Users should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

Intellectual Property and Copyright
Users should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that the user obtain all appropriate permissions before electronically publishing other people's work or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the Principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights. Users must not attempt to reproduce, distribute, transmit, publish, copy or exploit any material that constitutes an infringement of any intellectual property rights (such a copyright) of a third party; or in a way that violates any laws, such as privacy laws.

Computer Hardware
Computer facilities are expensive, sensitive and must be treated carefully. Users must not:

- Do anything likely to cause damage to any equipment, whether deliberately or carelessly
- Steal equipment

- Vandalise equipment (e.g. graffiti)
- Mark or deface any equipment
- Interfere with networking equipment such as hubs or fittings
- Attempt to repair equipment
- Unplug cables or equipment
- Move equipment to another place
- Remove any covers or panels
- Disassemble any equipment
- Disable the operation of any equipment

Users should report other people breaking these rules.

Regardless of the real or supposed levels of understanding, staff and students are NOT authorised to attempt the repair or adjustment of any College hardware or software. Any such attempt will be regarded as a violation of network security. Any problem with equipment or software must be referred to the IT Helpdesk.

Software and Operating Systems
Computer operating systems and other software must be set up properly for computers to be useful. Users will not:

- Change any computer settings (including screen savers, wallpapers, desktops, menus standard document settings etc) without permission
- Bring or download unauthorised programs, including games, to the College or run them on the College computers. Online internet games are banned
- Delete, add or alter any configuration files
- Copy any copyrighted software to or from any computer, or duplicate such software
- Deliberately introduce any virus or program that reduces system security or effectiveness
- Create or alter with any program, words or images which belittle any person

Networks
Network accounts are to be used only by the authorised owner of the account.

If you find a computer logged in, you should do nothing in that account except log out.

Users must not:

- Attempt to log into the network with any username or password that is not their own, or change any other person's password
- Reveal their password to anyone except the system administrator, or in the case of a student, their classroom teachers, only if necessary. Users are responsible for everything done using their accounts, and everything in their personal drive. Since passwords must be kept secret, no user may claim that another person entered their personal drive and did anything to cause the College rules to be broken
- Use or possess any program designed to reduce network security
- Enter any other person's personal drive or do anything whatsoever to any other person's files
- Attempt to alter any person's access rights
- Store the following types of files in their personal drive:
    - Program files (EXE, COM)
    - Compressed files (ZIP, ARJ, LHZ, TAR etc)
    - Obscene material – pictures or text

- Obscene filenames
- Insulting material, including demeaning words, or demeaning images which belittle any person
- Password-protected files
- Copyrighted material

- Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users

Printing
Users must always minimise printing by print previewing, editing on screen rather than on printouts and spellchecking before printing.

Students must not load paper into printers without permission. Paper that is pre-used, torn, creased, damp, irregularly shaped or sized or unsuitable for laser printers should not be used in laser printers.

Cyber-safety
If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent or caregiver as soon as is possible.

If a staff member believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must report it to the IT Helpdesk and inform their supervisor or the Principal as soon as is possible.

The College has developed a Student Anti-Bullying Harassment Policy (which includes cyber bullying) which all users must read, understand and comply with.

Internet Usage
Internet access is expensive and has been provided to assist in supporting students' education. Users must use it only with permission, and not in any unauthorised way. It is not intended for entertainment.

Because the internet is a continually changing environment, and not controllable despite the best intentions of the College, the College has a responsibility to ensure that, as far as possible, material obtained from the internet is not offensive or inappropriate. To this end, filtering software has been placed on the internet links. In the end, however, it is the responsibility of individual users to ensure their behaviour does not contravene College rules (or rules imposed by parents/guardians).

The College is aware that definitions of "offensive" and "inappropriate" will vary considerably between cultures and individuals. The College is also aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally and unintentionally, being obtained and displayed. If any inappropriate material is obtained, it is the user's responsibility to report this to their teacher or supervisor (as applicable) and the IT Helpdesk as soon as possible.

Web Filtering
The internet has become a powerful tool for teaching and learning, however users need to be careful and vigilant regarding some web content. To help protect users from malicious web activity and inappropriate websites, the College operates a comprehensive web filtering system. Any device connected to the internet through the College network will have filtering applied. The filtering system provides a layer of protection to users against:

- Inappropriate web pages
- Spyware and malware
- Peer-to-peer sessions
- Scams and identity theft

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content. The College's filtering approach represents global best-practice in internet protection measures. However, despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care but avoiding or reducing access to harmful information also requires responsible use by the user.

Users are required to report any internet site accessed that is considered inappropriate. Any suspected security breach involving students from outside the College's network must also be reported to the College.

It is conceivable that, especially for senior students, information is required for curriculum purposes that may appear to contravene the following conditions. In such cases, it in the responsibility of students and teachers to negotiate the need to access such sites.

The BYO devices have access to home and other out of College internet services and those services may not include any internet filtering. Parents and caregivers are encouraged to install a local filtering application on the student's device for when they are connected in locations other than College. Parents/caregivers are responsible for appropriate internet use by students outside the College.

Parents, caregivers and students are also encouraged to visit the Australian Communications and Media Authority's Cybersmart website for resources and practical advice to help young people safely enjoy the online world: https://esafety.gov.au

Users will not deliberately enter or remain in any site that has any of the following content:

- Nudity, obscene language or sexual discussion intended to provoke sexual response, pornography in any of its forms
- Violence and hate
- Information on, or encouragement to commit any crime
- Racism
- Information on making or using weapons, booby-traps, dangerous practical jokes or "revenge" methods
- Net cracking, security cracking, or anything that is invasive to personal privacy

If students encounter any such site, they must immediately turn off the computer monitor (not the computer itself) and notify a teacher. Do not show your friends the site first.

The internet must not be used for the following:

- Commercial purposes or profit
- Illegal purposes such as spreading computer viruses or distributing/receiving software that is not in the public domain
- It is inappropriate to act as though you intend to break the law e.g. by attempting to guess a password or trying to gain unauthorised access to remote computers. Even if such attempts are not seriously intended to succeed, they will be considered serious offenses

- Interactive use of the internet should ensure that there is no possibility of the transmission of viruses or programs which are harmful to another user's data or equipment
- Copyright is a complex issue that is not fully resolved as far as the internet is concerned. It is customary to acknowledge sources of any material quoted directly and it is a breach of copyright to transmit another user's document without their prior knowledge and permission. This includes the use of images and text. It is safest to assume all contact on web sites is the legal property of the creator of the page unless otherwise noted by the creator

Email

Electronic mail is a valuable tool for personal and official communication both within the College network and on the internet. Students and staff are encouraged to use it and take advantage of its special features. As with all privileges its use involves responsibilities.

Throughout the internet there are accepted practices which should be followed. The following points should be noted:

- Use appropriate language and be polite in your messages. Do not be insulting, abusive, swear or use vulgarities
- Never write hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours. No messages should contain obscene comments, threats, sexually explicit materials or expressions of bigotry or hate
- Do not reveal your personal address or the phone numbers to other users
- Note that email is not guaranteed to be private. System Administrators do have access to all files including mail. Messages relating to illegal activities may be reported to the authorities.
- Students and staff will control their own mail/web space on the internet server
- Use only the email service provided by Blackheath & Thornburgh College for College activities

A user will not:

- Log on to any mail server except that which is supplied to users by the College
- Send offensive mail
- Send unsolicited mail to multiple recipients ("spam")
- Use email for any illegal, immoral or unethical purpose
- Attempt to disguise their identity or the true origin of their mail
- Forge header messages or attempt to use any mail server for deceptive purposes
- Use any mail program designed to send anonymous mail

For further details, please also see the College Email Usage Policy.

School Responsibilities

The College acknowledges its responsibility to:

- Develop and implement this policy to ensure that the use of electronic devices by users does not disrupt others or the normal routine or running of the College
- Communicate this policy to students, parents and employees
- Keep appropriate records, monitor and report on any issues related to inappropriate electronic device use by users
- Encourage students, parents and employees to contribute to a healthy school culture

Employee Responsibilities
Employees have a responsibility to:

- Uphold the College's policy on this issue
- Take reasonable steps to prevent and respond appropriately to any instances of inappropriate use by students of electronic devices

Parent Responsibilities
Parents have a responsibility to**:**

- Read and understand, and ensure their child reads and understands, this policy before the student brings his/her devices to school
- Contact the College Reception on (07) 4787 5100 in cases of emergency. This remains the most vital and appropriate point of contact. Contacting students directly on their electronic devices during an emergency may create greater risk for students
- Uphold the College's policy on this issue
- Not engage in conduct prohibited by this policy or that otherwise disrupts others or the normal routine or running of the College

Student Responsibilities
Students have a responsibility to:

- Uphold the College's policy on this issue
- Not engage in conduct prohibited by this policy or that otherwise disrupts others or the normal routine or running of the College
- Report any breaches of this policy to their teacher, Head of School or the Principal

Monitoring and Reporting
Users should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

All material on the device is subject to audit by authorised College staff. If at any stage there is a police request, the College may be required to provide the authorities with access to the device and personal holdings associated with its use.

Staff and students must report any suspected IT security incident or breach to their teacher, the Risk & Compliance Officer, the Principal and the IT Helpdesk (as appropriate). If the incident involves a security breach, staff will need to follow the Data Breach Response Plan.

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

The College reserves the right to restrict/remove access of personally owned mobile devices to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to College supplied services.