NAMBOUR CHRISTIAN COLLEGE LTD

TECHNOLOGY (ACCEPTABLE USE) POLICY

College Policy 8.0

ISSUED	October 2003	**LOCATED**	T:\Admin\Policies NCC Website, Staff Portal, Parent Lounge, Student Café		
REVISED	29 July 2008	Reviewed 2015. No changes	April 2016. Minor changes	20 July 2016	16 October 2017
	11 Jan 23 Mobile phone section approved at Exec	Reviewed by IT - major changes Approved at Exec 15 Feb 2023	Approved at Board meeting 21 February 2023	March 2025	
REVISION SCHEDULE	Annually or as required		**APPROVED BY**	College Executive	
DOCUMENT OWNER/S	Head of IT				

POLICY

An important facet of the Mission of Nambour Christian College Ltd, herein referred to as the College, is to provide a secure and supportive Christ-centred learning community for every student. It is the Policy of the College that all information and technology usage aligns with the ethos of the College

In line with technological developments, the College recognises the need to provide access to online services that enable young people to be taught and acquire knowledge and skills for the 21st Century. Such "services" include all Information Communication Technology (ICT) and is not limited to the internet, intranet and electronic mail and devices.

The College is committed to providing access to ICT for all to support the teaching & learning program and administration of the College. The College provides access to these technologies underpinned by the expectation of safe and responsible behaviour by all members of the College community.

This Policy (available on the College website) should be read in conjunction with the Technology Warranty and Damage Guidelines (available on the Student Café and Parent Lounge). The policy applies to all forms of digital devices, connections and networks used and accessed, whether College owned or owned by students and all College owned devices and networks used and/or accessed on site or elsewhere.

The computers and computer network at the College together with access to the internet and email are provided for educational and professional purposes only. The use of these devices and network should therefore be consistent with that purpose, as detailed in this document.

Users who are in doubt about whether certain behaviours are within the standards should refer the issue immediately to the Head of IT.

The principles of behaviour relating to the use of school resources include respect for the law; respect for other people; and respect of the College's mission and values. The principles of conduct also assume integrity, diligence, economy and efficiency from the users. This policy covers all technology devices which are used at school, including those provided by the College and those which are brought in externally by staff and students (BYOD).

PROCEDURE

For students, the following documents should be read in conjunction with this policy:

- IP&P 35.0 T6 Technology (Acceptable Use) Guidelines for Students
- IP&P 36.0 T7 Technology Warranty & Damage Guidelines
- The abridged Technology Policy and Procedures in the Enrolment Contract

1. Definitions

Mobile Device is inclusive of mobile phones and smart watches.

Information and Communication Technologies (ICT) is any electronic device or related applications which allow users to record, send, access or receive information, in textual, audio, image or video form.

These may include but are not restricted to:

- Computer systems and related applications such as email and internet
- Web-based tools such as discussion forums, chat rooms, blogs, podcasts, internet social networks and instant messaging systems
- Mobile devices such as mobile phones, tablets, and wearable devices
- Fax machines and scanners
- Output devices such as printers
- Imaging tools such as video or still cameras
- Audio tools such as audio recording devices.

Users refers to all board members (herein, considered staff), employees (staff), contracted workers, students and parents at the College.

2. Legal Implications

For legal purposes email has the same standing in court as paper documents. Users must be aware that the College can be involved in litigation. Records relating to use and activities involving email, internet and intranet can be requested by a court order or subpoena. These include matters affecting legal proceedings, affecting personal affairs of employees, parents, students, or third parties, as well as relating to research, or other communications even if communicated in confidence.

Emails residing on or transmitted across the Nambour Christian College computer system are the property of the College. All electronic files are the property of the College, and users should act on the basis that they can be, and where necessary will be, held accountable for their messages and stored files.

While all transmissions remain the property of the College by law, all efforts to retain professional confidentiality will be made. Confidentiality is not guaranteed regarding private emails that are sent/received on the College system. All internet activity is recorded for individual users. Reports of this activity are continually being monitored. Filtering and monitoring of online activity will occur at periodic intervals without prior notice.

Specifically, for Students:

Where there is an alleged criminal offence or serious disciplinary matter concerning a student, the individual concerned will generally first be told the circumstances of the grievance. Parents will be informed, and disciplinary actions taken. The College reserves the right for any reason whatsoever to inspect without forewarning any files, information or logs held on any College computer or service

Specifically, for Employees:

Should access to an individual's files or internet logs be necessary for an alleged criminal offence or serious disciplinary matter the individual concerned may be told the circumstances of the complaint prior to the files or logs being accessed. This will be done by the Head of IT when requested by the NCC Executive. The College reserves the right for any reason whatsoever to inspect without forewarning any files, information or logs held on any College computer or service.

3. Classroom Requirements

Specifically, for Students:

- Bring an acceptable learning device (which has previously been charged) to each lesson unless otherwise instructed. This should be the device supplied by the College
- Maintain confidentiality of personal username and password
- Comply with the instructions of teachers
- Conform to acceptable school behaviour, conduct and standards
- All devices can only be used when inside classrooms and/or under the supervision of the classroom teacher. Any use during morning tea, lunch, before and after school must be done in the library
- Refrain from bringing data storage media, (eg. USBs, CDs, etc) into the computer rooms or library unless required for keyboarding or document transfers
- All work and documentation should be backed up regularly to Onedrive to prevent loss or corruption of files
- Ensure that, when required, data storage media is virus checked prior to reading from or writing to it
- Ensure the College supplied devices with smart pens have the pen safely stored all times to ensure they are not lost
- Ensure the device is kept in the College provided bag / case at all times when the device is being transported or not being used
- Use headphones only during times deemed appropriate by the classroom teacher
- The process for replacing a lost or damaged school device is detailed in the technology warranty and damage guidelines
- Never access another person's computer folders
- Do not use technology in any manner or place that is disruptive to the normal routine of school activities eg class, sport, chapel, assembly or public functions
- Honour the agreement in the enrolment contract that was signed
- Adhere to the acceptable use agreement when using the device, both at home and at College, including during lunchtime or when not in the classroom.

Specifically, for Employees:

- Ensure that students have clearly defined tasks for using the on-line services and resources
- Provide appropriate levels of supervision
- Educate students about intellectual property and copyright laws
- Provide students with an ethical understanding of the issues regarding plagiarism
- Educate students about the information handling skills of on-line research, including evaluating, verifying and citing the on-line sources of their information
- Educate students in locating suitable resources available through catalogues, directories and teacher developed resource lists, and also when to use search engines.

4. Acceptable Use Parameters

4.1. Appropriate activities include

- Only accessing and storing appropriate content
- Connecting to resources that provide a variety of academic and/or employment related information
- Exploring the internet looking for information and resources useful in carrying out academic and professional requirements
- No messaging services are approved for use by students on College devices or networks.

Specifically, for Students:

- Email and communication between students using the device should be for educational purposes only.

Specifically, for Employees:

- Minimal amounts of personal correspondence with family or friends.

5. Unacceptable Use

5.1. Sharing passwords and logins

- Users must not pass on their login code or password to any other person, with the exception of IT employees only in exceptional circumstances. Students are not to share their passwords with teachers. Staff are not to share their passwords with students or other staff.
- Students are not to log into staff devices, and staff are not to log into student devices. This is to protect the elevated level of access available to staff.
- Devices are to be locked or logged out when staff are not at their computers. This must be done every time you step away from your device when it is not in use
- All programs are to be closed when not in use
- Staff are not to send their device across the campus with another person (for example, to IT for support) with the device logged in or password written. If this happens, the staff members credentials will be reset without notice, and the staff member will be required to visit IT to have them set again to maintain security and integrity of the College information.

5.2. Damage

- All devices being presented to the IT Department for repair or upgrade must be accompanied by the designated owner of that device, and never via a third party
- Users must not damage computers, computer systems or computer networks. This includes removal and/or swapping of keyboards and/or other computer components, including software.
- Undue rough handling of computer and/or peripherals
- Stylus pen not securely stored to prevent loss
- Protective case removed from the student device when the device is not in use
- Deliberately damaging or modifying equipment
- Stealing or destroying equipment, software or data belonging to the College, other users or other entities (including web based)
- Presence of food and drinks around the computer, including when it is in a school bag. Do not consume food or drink while using the computer
- No graffiti or stickers are to be put on the device
- Be aware of the location of school bags while the device is inside. School bags containing devices must be in an undercover protected area, or in a school locker
- College stickers must not be removed from devices. This will be considered a form of damage
- Device is not to be used on wet or dirty surfaces
- Further information relating to damage to devices and the associated fees for repairs and rectification of damage can be found in the following documents:
  - Technology (Acceptable Use) Guidelines for Students
  - Technology Warranty and Damage Guidelines

5.3. Defamation

Users must not publish, post or include in an email any material which might be deemed to defame, denigrate or humiliate an individual, company or organisation.

5.4. Improper communications

- Such as chain letters or harassing mail. Sending of improper communications may harm Users and expose the College to risk of legal action or adverse publicity. Emails must not be sent anonymously and must include a signature block.
- Use of vulgar, derogatory or obscene language while using technology at school to communicate will result in disciplinary action as directed by the Executive Principal.

5.5. Social media, photos, commercial and other inappropriate use

- Use of the College devices/network/email for personal financial gain, gambling purposes or advertising is prohibited

- It is forbidden to use technology to capture audio, take videos and/or pictures of staff and students of the College without their consent. This does not include the use of College security CCTV footage or other footage that the Executive agrees is for student, staff or facility safety
- It is forbidden to use non-College owned devices to take pictures of students, unless permission has been granted by Line Managers for specific reasons
- When permission has been granted, photos taken using personal devices must be uploaded to either Pixevety or the College T Drive as soon as reasonably possible and delete these photos from the personal device immediately after this, including any recycle bins or cloud linked spaces
- Communication between staff and students must be schoolwork related and must only take place via the College email network or Microsoft Teams and not by personal email addresses, social media, messaging platforms, or other electronic means
- All forms of social media are inappropriate for use during the school day
- All staff are forbidden to have social media connections with current students without exception.

5.6. Harassment

Users must not transmit, or cause to be transmitted, communications (whether in the form of text, picture or other data) that may be construed as harassment or disparagement of others based on the criteria of the anti-discrimination legislation and College policy. It should be noted that it is a criminal offence to use technology to menace, harass or offend another person. As such, the College may consider it appropriate to involve the Police.

5.7. Jokes

Users must not send emails which contain jokes and/or articles which are in poor taste, contain coarse language, racist or sexist comments.

5.8. Pornography

Users must not access, store or transmit pornographic material on College systems. When such material is inadvertently encountered, the employee or student must immediately exit from that site and advise either, their teacher, the Head of IT or another College staff member. If this site has implications for searches, the Head of IT must be advised of the unwanted site link.

5.9. Inappropriate use

Includes, but is not limited to the following:

- Access, use or distribution of confidential student or staff information that doesn't relate to a user's official role at NCC. For example, a teacher or Teacher Assistant might have access to confidential notes about a student (their own child or family friend, etc). Under no circumstances is this information to be accessed, used, or distributed if it doesn't directly relate to the user's role at NCC. Any inappropriate use of data will be heavily disciplined.
- Infringe the copyright or other intellectual property rights of third parties. Students should not download and use work without the express permission of the owner.
- Download software, unless appropriate authorisation and compliance with licensing requirements and established policies to check all such software for computer viruses is followed.
- Disrupt communication and information devices through such means as mass emailing or transmitting files which place an unnecessary burden on departmental resources.
- Access inappropriate internet sites (see 6.10. Inappropriate Internet Sites below).
- Download, distribute, store or display offensive or pornographic graphics, adult sites, images or statements or other material obtained from inappropriate internet sites.
- Access and/or distribute material that is discriminatory or could cause offence to others, for example, offensive material based on gender, ethnicity or religious or political beliefs.
- Download material for non-work related or non-educational use.
- Download information for the purpose of providing it to external organisations or the general public without authorisation.
- Distribute chain letters.
- Distribute defamatory, obscene, offensive or harassing messages.

- Distribute confidential information without authority.
- Distribute messages that disclose personal/sensitive information without authorisation.
- Distribute private information about other people.
- Distribute messages anonymously, using a false identity or using another person's email account.
- Engage in any illegal or wrongful activity.
- Download/supply to others inappropriate site addresses.
- Knowingly engage in any activity which may compromise the security of the local area network, intranet or external network.

5.10. Inappropriate internet sites

Inappropriate sites include, but are not limited to, sites that:

- Are illegal
- Are pornographic or contain inappropriate or obscene sexual material
- Advocate hate/violence
- Contain discriminatory material, e.g. Based on gender, race, religious or political beliefs; and offer inappropriate games or software
- Are deemed by the College to be inappropriate.

6. Consequences of Unacceptable Use

Specifically, for Students:

Where there is an alleged criminal offence or serious disciplinary matter concerning a student, the individual concerned will generally first be told the circumstances of the grievance in discussions with RTC or Deputy HOJS. Parents will be informed, and disciplinary actions taken. The College reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any College device. Serious misuse will be resolved under the guidelines of the Suspension and Exclusion Policy, the Student Bullying Policy and Child Protection Policy and may result in notification to the Police.

The College has determined three levels of breaches in relation to this policy. These are defined in the policy:

- Technology (Acceptable Use) Guidelines for Students

Specifically, for Employees:

Should an employee breach the Technology (Acceptable Use) Policy, it may lead to disciplinary action, up to and including termination of the employment contract.

Should access to an individual's files or internet logs be necessary for an alleged criminal offence or serious disciplinary matter the individual concerned may be told the circumstances of the complaint prior to the files or logs being accessed. This will be done by the Head of IT when requested by the NCC Executive. Notwithstanding the above, the College reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any College computer.

7. Mobile Device Use

The College accepts no responsibility for replacing lost, stolen or damaged mobile devices. This includes travel to and from school.

If communication is necessary, parents can contact their child/ren through the Junior and Main Reception.

Where a student is allowed/required to bring a mobile device to school, the following applies:

- Mobile phones are not to be visible or in use during school hours.
- Smart watches are not to be worn during school hours.
- On occasion, teachers may permit students to use their mobile phone during class time, for educational purposes only.
- Earphones must not be connected to a mobile device either directly, or via Bluetooth. Note: earphones are allowed to be connected to a school issued laptop for educational purposes.

- Mobile devices are not to be used at the Café for the purchase of food (effective from beginning Term 2, 2023).

The following consequences apply, should a student use their mobile device without teacher permission:

- Students will be directed to the Student Office in Middle or Senior School or their classroom teacher in Junior School to hand in their mobile device where it will be collected by the student at the end of the day
- Students will then be directed to the RTC or RTO for a Mobile Device Plan to be completed
- Should a third offence occur in a calendar year, the mobile device can only be collected by a parent at a time convenient to them
- Subsequent breaches after the third offence, are considered to be a serious offence and will activate the Suspension and Exclusion Policy.

Should students be required to make calls or check text messages during school hours, this can ONLY be done either under the direct supervision of a teacher during break times, or at the Student Office with permission from the staff member at the desk.

All Middle and Senior School students are encouraged to keep their mobile device in their lockers, and Junior School students must keep their mobile device in their bag.

All students are to be discreet with their contact details as these should be regarded as private, thereby protecting themselves from unpleasant, threatening or abusive texts and/or images.

8. Privacy Issues

Users must not include in documents or emails personal information about colleagues, students or parents without their written consent. Employees and students should act within the Privacy Policy of the College. Employees and students are not to use NCC ICT in any way that could bring the College into disrepute.

College data and information must only be stored on approved systems and College issued devices.

College data and information must only be accessed using College issued devices. This includes data and information that is accessed externally while the user is not on College grounds. In some cases, certain information from web-based systems will be accessible on personal devices (Such as Payroll, TASS, etc) which is acceptable, however, information in relation to staff, students and parents is not to be downloaded onto these devices. (Such as a class lists, student contact information, or academic results).

Any personal or sensitive data or information stored on a device must be deleted when no longer required.

All electronic correspondence and other electronic documents regarding personal or sensitive information must be filed in a secure location in the College storage systems. Only authorised staff will have access to this information. Authorised employees may only access these files for authorised purposes.

Any printed material which contains personal or sensitive information about staff, students or parents is to be stored in a locked storage facility and must be destroyed when no longer required.

All College data and information that is removed from College grounds by any means (USB drive, printed, personal device) must be deleted or destroyed once it has been used.

If you become aware of a potential loss of data (data breach) in instances such as

- An email sent to the wrong recipient containing Personal Identifiable Information
- A USB or external storage device being lost or stolen containing Personal Identifiable Information
- A printed copy of Personal Identifiable Information being lost or stolen
- A work or personal device being lost or stolen that contains Personal Identifiable Information.

You are to immediately contact the Head of IT and/or the Head of Business Operations to report this so a determination can be made on the nature of the breach. Personal Identifiable Information is anything that contains the information of staff, students or parents.

9. Forums

Only employees of the College may subscribe to listservs, however they need to:

- unsubscribe or suspend mail from listservs during holiday periods and periods of absence
- be familiar with and follow the common rules of etiquette of that listserv
- include a signature block in all postings
- delete unwanted emails.

10. Copyright

Users must not:

- Download or authorise downloading of information or software from the internet or emails to provide to a third party
- Violate copyright, license agreements or contract of usage
- Undertake any action which might interfere with the integrity of data or a commercial software program.

11. Respecting the Systems' Limitations

Users are requested to:

- Avoid sending large attachments, or other large distribution lists because of the impact on the network's performance
- Not send, forward and/or reply to large distribution lists concerning non-school business
- Must consider the impact on the network when creating and using large distribution lists
- Not forward lengthy or frequent emails to system groups, which may be time-wasting or unwanted for many recipients.

12. Protection Against Viruses

Users need to work in accordance with safe computing practices to minimise the risks associated with computer viruses.

Note:

- Be careful opening email attachments from unknown sources; if in doubt about a source, check with the IT Department
- Never open .exe files
- Should the virus protection software detect a virus from an incoming file, inform the person who introduced that file so they can ensure it does not happen again and inform the IT Department
- If a device is acting in an unexpected manner, there may be an undetected virus. Whilst this is not common, if this does happen notify the IT Department immediately
- Users must not open attachments or click on links in an email unless they have confirmed the validity of the attachment or link with the sender
- If any suspicious emails, attachments and links are received, the IT Department must be notified immediately
- Users must make all efforts to validate the identity of the user (by checking the email address, name and the external sender bar on the email) before sending any email replies.

13. Staff BYOD Devices

NCC provides staff access to the **C**ollege WIFI for personal (BYOD) devices for personal use or to access WIFI calling when signal in parts of the school is **below standard**. This service is provided by the College with no expectation of it functioning with all devices and the College reserves the right to restrict or deny access to certain devices.

All BYOD devices will not **have and** will not be provided access to core NCC services such as T drive or printing with no exception and must be free of viruses and malware. No NCC Personal Identifiable Information is to be downloaded onto these devices.

Students are not permitted to join personal BYOD devices to the College network, and thus staff are not to provide their username and password to students for this purpose. Accounts will be **suspended,** and disciplinary action will be taken if this happens.

14. Software Use in College

Only NCC approved software is to be used in the College. This includes web-based applications. This is required to ensure the protection of College data of staff, parents, and students as well as ensure we are licensed appropriately according to the terms and use of individual software.

If a department in the College wishes to obtain or trial new software, the first step is to contact the Head of IT to discuss requirements, logistics, and budget. Staff are not to engage with software vendors prior to this taking place, and especially are not to sign contracts with vendors under any circumstance.

All software requests will be approved/rejected on a case-by-case basis with an explanation provided for the reason of the decision.

Any department or staff found to be using non-approved software and/or uploading student information to these systems will be asked to why they haven't followed process and potentially have access to these platforms immediately removed until further notice.

15. Conservation of Electronic and Print Resources

Efforts must be made to conserve the finite resources of the College. This can be achieved through such behaviour as:

- Avoid using large amounts of the system resources such as disk space
- Avoid leaving programs open causing congestion of the network. All programs should be closed when not in use
- Always close down properly, avoiding system failures
- All documents must be saved regularly to OneDrive;
- Avoid printing straight from an internet site. Copy and paste the relevant section or use a database to keep track of your data
- Endeavour to keep paper wastage to a minimum
- Before printing, proofread, spell check, and print preview your document, and only when completely satisfied with document send it to the printer
- Place unwanted printouts in recycling boxes.

16. Personal Responsibility for Security

System security is the individual and collective responsibility of all users. All suspected security violations will be treated seriously as they may threaten the provision of the College service. Any user who suspects a security problem on the school network including the internet must immediately notify The IT Department and not demonstrate the problem to others. Any user who believes their files have been tampered with must immediately change their password and contact the Head of IT with the specific details.

The College reserves the right to disable any user account at any time without notice if it is suspected that their account has been compromised, or if they perform any actions which are in breach of this Policy.

17. CCTV Statement

The College has multiple CCTV cameras installed around the College. These are in place for security and safety reasons only, but will be used to assist in identification of individuals, on request from the College Executive and in consultation with the Head of IT.

Other staff may request access from the Head of IT or the College Executive to the data from these cameras, and limited access may be granted for the purposes or security and safely of individuals and property.

The CCTV cameras cannot be accessed offsite. Only the Head of IT and the Property Manager will be able to access this footage remotely.