TECHNOLOGY (ACCEPTABLE USE) POLICY

ISSUED	October 2003	LOCATED	T:\Admin\Executive\1.College Policies - All major College policies\College Policies		
REVISED	29 July 08	Reviewed 2015. No changes	April, 2016. Minor changes	20 July 2016	16 October 2017
	11 Jan 23 Mobile phone section approved at Exec				

1. Overview

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.

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

Any employee or student, herein referred to as Users, who is in doubt about whether certain behaviours are within the standards should refer the issue immediately to Head of Computing or IT Coordinator. Users are to maintain healthy relationships, netiquette and demonstrate Christian character when using technologies.

The principles of behaviour relating to the use of school resources include: respect for the law; respect for other people; and respect of the Nambour Christian 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 student owned.

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

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

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 or logs held on any College computer.

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 will generally first be told the circumstances of the complaint and will be requested to be present when the files or logs are opened. The individual may be accompanied by their Union representative, or a colleague. The College reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any College computer.

3. Classroom Requirements

Specifically, for Students:

- bring an acceptable learning device to each lesson unless otherwise instructed. This should be the device supplied by the College
- maintain confidentiality of personal username and password
- comply with 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 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 attached securely to the device at all times
- ensure that the keyboard covers the screen at all times when not in use, especially when moving between classes
- Ensure that the protective case provided by the school remains on the device at all times
- 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 Student Technology Warranty and Damage Guidelines
- never trespass in another person's computer folders
- 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 they have signed

Specifically, for Employees – teaching staff:

- 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

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
- school-based or authorised IRC (internet relay chat) and discussion groups.

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. An average of 10 minutes a day on non-employment related emails is a guide.

5. Unacceptable Use

Sharing Passwords and Logins

- Users must not pass on their login code or password to any other person, with the exception of IT employees or students to teachers
- When not at your computer, log off.

Damage

- 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.

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.

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. Email must not be sent anonymously, and must include a signature block.
- Use of vulgar, derogatory or obscene language while using technology at school will result in disciplinary action as directed by the Head of College/School.

Social media, commercial and other inappropriate use

- Use of the College computers/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.
- Communication between staff and students must be school-work related and must only take place via the NCC email network and not by personal email addresses.
- All forms of social media are inappropriate for use during the school day.
- Teachers are forbidden to have social media connections with current students.

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.

Jokes

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

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, Head of Computing or IT Coordinator. If this site has implications for searches, the Systems Administrator must be advised of the unwanted site link.

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. 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 computer. Serious misuse will be resolved under the guidelines of the NCC Suspension and Exclusion Policy, the College 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 Technology (Acceptable Use) Guidelines.

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 will generally first be told the circumstances of the complaint and will be requested to be present when the files or logs are opened. The individual may be accompanied by their Union representative, or a colleague. 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 Phone Use

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

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

Where a student is allowed/required to bring a mobile phone 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 phone either directly, or via Bluetooth. Note: earphones are allowed to be connected to a school issued laptop for educational purposes.

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

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

- Students will be directed to the Student Office to hand in their mobile phone where it will be collected by the student at the end of the day.
- Students will then be directed to the RTC for a Mobile Phone Plan to be completed.
- Should a third offence occur in a calendar year, the mobile phone 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 phone in their lockers, and Junior School students must keep their mobile phone 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.

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 e.g. introduce viruses.

11. Respecting the systems' limitations

Users are requested to:

- avoid sending large attachments, especially to the address, 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
- avoid the use decorative email screens.

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 IT personnel
- 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
- if a computer is acting strangely, there may be an undetected virus. This does not happen often, but it is worth checking with the network team.

13. Conservation of electronic and print resources

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

- avoid using large amounts of the system resources such as disk space
- avoid leaving programs open causing congestion of the network
- always close down properly, avoiding system failures
- avoid waste such as unnecessary broadcast messages or attaching large files to messages
- avoid printing straight from an internet site. Try to 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
- email received on the College system is retained on the server until deleted by the recipient.

To conserve disk space, maintain your mailbox by:

- keeping messages short
- checking email daily
- deleting unwanted messages immediately
- emptying your deleted messages wastebasket frequently
- saving wanted messages to file rather than leaving them in the mail.

14. Personal responsibility for security

System security is the individual and collective responsibility of all ~~College~~ 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 Principal 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 School with the specific details.

15. 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 Head of College or his representative, if necessary.

16. Review

This policy will be reviewed each year, or as required.