ST. JOHN'S
CLIFTON HILL

INFORMATION AND COMMUNICATION TECHNOLOGIES POLICY

RATIONALE

St John's School believes that the benefits for students and staff to access Information and Communication Technologies (ICT) far exceed any inherent risks. These benefits include access to global and up to date information resources, opportunities for collaboration, both within the School and with the wider community, and personalised learning.

St John's School recognises that:

1) ICT plays an increasingly important role in the students' learning and the creation and delivery of curriculum by teaching staff.

2) The establishment and implementation of an acceptable use policy, guidelines, resources and user agreements for students / parents / caregivers, and administrative / teaching staff:

a) ICT contributes to the provision of a safe learning environment and addresses the emotional, physical and social development of students.

b) ICT contributes to the maintenance of a safe working environment

c) ICT assists St John's to meet its obligations to deliver a curriculum in manner that is consistent with the School's values, beliefs and mission.

3) For the purpose of this policy, ICT includes, but is not limited to:

- Computers and the school network
- Internet
- Mobile phones
- Wireless Devices
- Personal music devices including MP3 players
- Recording devices
- Portable storage, including USB and flash memory devices

4) The ICT Policy provides staff and students with the opportunity to use these technologies appropriately to enhance teaching and learning in a safe physical and emotional environment.

5) The use of the St John's School computer network, internet access facilities, computers and other technological devices should be for educational or professional purposes. The use of privately owned technological devices or equipment on the School site or at any school related activity must be appropriate to the school environment and in accordance with the guidelines of this policy.

6) It is an expectation that staff and students will use ICT facilities and equipment appropriately at all times.

7) Every reasonable attempt will be made by the School to filter out any inappropriate material to maintain a safe physical and emotional environment.

PURPOSE

To ensure all staff and students of St John's School are accessing and using information and communication technologies in an acceptable manner in accordance with our School Vision, other relevant policies and the laws of this Country and State.

SCOPE

This ICT Policy applies to all users who access the School Network by whatever means and those who use School owned or leased equipment.

AIMS

1) To communicate the acceptable use of ICT to staff and students.

2) To communicate an individual's rights and responsibilities when using information and communication technologies.

3) To ensure that all users take appropriate precautions when using information and communication technologies including the protection of passwords and safe transport and storage of equipment.

4) To ensure the security of data on the St John's School network or other technological devices.

5) To promote appropriate and lawful use of ICT when accessing, copying, using and distributing data.

6) To ensure that information and communication technologies are not used to facilitate inappropriate or illegal behaviour.

RIGHTS AND RESPONSIBILITIES

1) Each user is held responsible for his or her actions when using ICT. Inappropriate use will be dealt with through suspension or withdrawal of privileges and may also attract penalties under State and Federal laws. Examples of inappropriate use include any activity that:

- Violates or infringes the rights of another person, including their right to privacy.
- Initiates access to or transmits inappropriate or illegal material, including material which contains real or potentially defamatory material, false, inaccurate, abusive, obscene, violent, pornographic, profane, sexually-explicit, sexually-oriented, threatening, racially offensive, or otherwise biased discriminatory or illegal or any other inappropriate material

- Violates copyright.
- Violates any other school policy. (e.g. Harassment Policy)
- Transmits personal views on any matter, or views purporting to be or potentially seen to be views of the School.
- Places images, text or audio-visual content of a member of the school community on the school network or any global information system (e.g. social networking sites) without the express permission of the person depicted, or their guardian or caregiver where appropriate.
- Fails to use the system as prescribed in this policy and thus permitting infection by computer virus either deliberately or inadvertently.
- Results in unauthorised external access to the school's electronic communication system.
- Involves the unauthorised installation and/or downloading of any material or software that has not been approved by the School.
- Involves unauthorised repairs.
- Offends or potentially offends the ethos, principles and/or foundations of the school and or Catholic teachings.
- Wastefully uses finite resources.

2) If a user suspects that someone else is aware of his/her network or intranet password, they may alter such passwords or request that the responsible administrator ensure that such passwords are altered.

3) In the event of accidental access of inappropriate material, users should:
- Not show others.
- Close or minimise the window.
- Report the incident immediately to an appropriate person.

DEFINITIONS

Acceptable Use refers to common sense, decency and legal responsibilities applied to the Network and the writing of emails, messaging, documents, use of a camera facility and downloadable audio and video footage. Users must accept that at St John's School, the primary use of ICT is for educational and professional purposes.

Downloads refers to the downloading of software or the downloading of audio or visual material from the internet and/or physical devices such as mobile devices and memory sticks.

Email refers to all technologies used to transfer electronic messages, including email from one computer to another; instant messaging and peer-to-peer file exchange.

Internet means the worldwide communication system of interconnected networks and computers which connects people through their computers.

Network Administrator means the person/s appointed by the School to manage and supervise the Network and all related equipment. The Network Administrator has special rights of access and control that are not available to other users and are intended to guarantee the integrity and security of the Network.

Network means the School's computer network which includes access to the intranet of the School, the global Worldwide Web through the Internet, email, software, file/data information and hardware.

The School refers to St John's School, Clifton Hill and its authorised officers.

Unacceptable use refers to any use that:

- violates the beliefs, values and policies of the School
- violates the law of this Country and State (including the Privacy Act 2000)

User means a person authorised to use the Network. This includes students, staff, parents, caregivers and other persons authorised by the School.

User Agreement refers to the agreement that St John's School students, staff and other authorised users sign when they request access to the School's ICT.

PROPRIETORY RIGHTS

The contents of the St John's School network, including emails, materials developed using School facilities and equipment or materials downloaded to the network, remain the property of St John's School.

PASSWORDS

1) Users are advised to make passwords as strong as possible through a combination of numbers, letters and symbols; these should be a minimum of 5 characters in length with a combination of upper case and lower case.

2) Passwords must not contain obscene or inappropriate language.

3) Users should endeavour to keep their passwords confidential at all times.

4) Users are advised to not disclose passwords to any other person.

5) Users are not permitted to share passwords in order to use school network facilities.

6) If a user suspects that someone else is aware of or is using their password, they should immediately change the password.

NETWORK USE

1) Software should not be installed to or copied from the School network without the permission of the Network Administrator. This is to ensure that the school has the appropriate licences to the software.

2) Archival material on all drives should be burnt to CD or DVD or an external storage device and deleted from the Network periodically (i.e. each semester). An external hard drive is permissible for back-up purposes.

3) A student drive ('Z' drive) is available for staff and students to share information.

4) A staff drive ('N' drive) is available for staff to share information for staff use only.

5) An administration drive ('L' drive) is available to those with Administration rights and responsibilities.

6) Users should not attempt to access network drives not assigned to them.

USE OF EMAIL

1) Email is a major means of formal communication between staff, students, parents and the wider community

2) The use of email should be consistent with the mission, goals, policies and values of the School.

3) Users are encouraged at all times to exercise care when creating email messages. Appropriate/acceptable language, data and pictures should be used with care and consideration in email messages.

4) The intended audience of the email needs to be kept in mind when constructing the content of the email to ensure the appropriate level of formality or informality and structure of the document.

5) Users are encouraged to not reveal personal details or information in an email as this can be easily forwarded to recipients they don't know – email is inherently not secure.

6) Users should ensure that messages are addressed to the appropriate recipient.

7) Users should not use email in an unacceptable manner as defined by this document in Definitions.

8) Emails emanating from members of staff will contain the following notice to advise the receiver of potentially confidential or sensitive material and also to ensure that the recipient is aware that what is stated is not necessarily reflective of the School position:

> *This e-mail and any attachments may be confidential and if you are not the intended recipient you must not disclose or use the information in this mail. If received in error, please notify us immediately by return e-mail or by calling 03-9489-1346 and then delete the e-mail and all copies. St John's School, Clifton Hill, does not guarantee that this e-mail is virus or error free. The attached files are provided and may only be used on the basis that the user assumes all responsibility for any loss, damage or consequence resulting directly or indirectly from the use of the attached files, whether caused by the negligence of the sender or not. The content and opinions in this e-mail are not necessarily those of the school.*

9) The following are prohibited:

- "Spamming" or sending unsolicited commercial electronic messaging in accordance with the SPAM Act 2003 (Sending junk, unwanted mail via email).
- "Spoofing" or deliberately changing the "sender" field of email.
- Other practices contrary to the spirit and intent of this policy.

10) If a user receives a suspicious email, then the user should immediately delete the email from the Inbox and the Trash box. If unsure always contact an administrator before opening the document or other attachment(s).

11) Email attachments being sent should be limited in size. Large files (containing multimedia content) should not be sent via email. Users are reminded that there is currently an 11Mb limit on email size including attachments. Users should also be aware that it is not currently possible to forward emails approaching 5Mb using the School system.

12) Use of Gmail, Yahoo and Hotmail (or any other third party email service) on school equipment must follow the same protocols as school email accounts.

13) Access to Email accounts is only available through the School intranet except on certain Administration accounts that employ Outlook or SAS to manage the volume of messages received and sent.

INTERNET USE

1) As notified in the schools Privacy Policy, the school may use cloud based storage for both backup and storage of data and student work. It should be noted that Google Apps for Education (GAFE) uses cloud based storage which may be on servers located overseas. Please also note confidential and sensitive data is stored on the school server and not uploaded to overseas cloud servers.

2) Users can gain Internet access once they have logged into the Network using staff computers and student notebooks. Network login is not necessary for student Chromebooks and iPads but student history is regularly reviewed on these devices where deemed appropriate or necessary.

3) The Network Administrator may from time to time monitor the volume of Internet activity by users and the sites used by users. Users should be aware that Internet usage is logged and any concerns advised to the Principal.

4) The use of the Internet should be consistent with the mission, goals, policies, values and beliefs of the School.

5) Users should be aware that any software, games, music or movies downloaded from the Internet should be able to be used legally by the School. If a user is unsure of the licensing of Internet downloads, then they should speak with the Network Administrator. This is to ensure that the school has the appropriate licences to the software, games, music or movies.

6) The School employs Internet blocking software. However, users should be aware that blocking software is not 100% secure.

7) If a student or staff member comes across an inappropriate/ unacceptable site, they are asked to inform the Network Administrator who can manually block the website address.

8) All computers at St John's School have antivirus software installed and automatically updated.

9) If a User becomes aware of, receives or gains access to a virus, the user should immediately contact the Network Administrator for advice on what to do.

10) St John's School has secure hardware and software firewalls to stop intrusions. Access to the Internet is limited by filters controlled in part by the CECV and in part by the School to prevent access to inappropriate material.

11) St John's School has an external hard-drive based back up system for the whole network. The external hard-drive is rotated at a minimum every 14 days with the spare kept off-site.

12) Users are asked to notify the Network Administrator immediately if they become aware of any incident that could affect the security of the Network or related data.

SURVEILLANCE AND PRIVACY

1) The School encourages the use of electronic communications and respects the privacy of users. It does not routinely inspect, monitor or disclose email communications without the request of the Principal or Parish Priest.

2) From time to time the Network Administrator will be required to conduct an audit to ensure that the School's facilities, resources and services are all being used appropriately and comply with the law and school policies.

INTELLECTUAL PROPERTY/COPYRIGHT

1) Users must only use software on St John's School machines that is licensed to the School.

2) Users should respect the intellectual property rights of others. In particular, users should be conscious of the provisions of the Australian Copyright Act.

3) All texts, photographs, video clips, audio clips, music, movies, games and computer software are protected by copyright. Unauthorised copying, distribution or downloading of this type of material can constitute breach of copyright.

4) Any material downloaded from the internet needs to be cited fully in any work submitted by a student or disseminated by a member of staff or other authorised user.

HARDWARE

1) All computer facilities, including notebook computers, desktop computers, scanners, printers, and digital cameras (both still and moving) are expensive, sensitive and must be treated carefully by all users.

2) Users are asked to forward all repairs or problems with hardware to the Network Administrator promptly. Please do not attempt to repair equipment yourself as this is in breach of the insurance policy.

STUDENT ACCESS

1) Both during and outside class time, students should take responsibility for their own use of the Network and ICT facilities and equipment. Teachers play a supervisory role in the class room but the ultimate responsibility rests with the student. Parents and caregivers should remain vigilant regarding their students' use of information and communication technologies outside of class time.

2) Parents and caregivers share with the School the responsibility for setting and conveying the standards that students should follow when using information and communication technologies.

3) The School will undertake regular information sessions and relevant lessons for students, parents/caregivers and members of staff on acceptable and appropriate use of information and communication technologies. This will include but not be limited to recommendations for ensuring personal safety and security are maintained both within the school and in the wider school community.

BREACH OF THIS POLICY

In accordance with this policy and the relevant User Agreement, breaches of either will be dealt with on a case by case basis. Disciplinary action will be decided by the Principal or the relevant member of staff in consultation with the Principal.

MOBILE PHONE

1) The School recognises that there are times when it is appropriate and useful for students to have access to a mobile phone – for example, to contact parents in emergencies outside of school hours. However, it is neither necessary nor acceptable for mobile phones to be switched on or used during school hours. As such, the device should be handed in at the office for safe keeping during these times.

2) It is the responsibility of students who bring mobile phones to school to adhere to the guidelines outlined in this policy in regard to ICT devices, applications and appropriate use.

3) Where parents or caregivers decide to provide a student with a mobile phone, they should make the student aware that the use must not breach school policies.

4) Parents and caregivers are responsible for advising the school in writing that a pupil is permitted to carry a mobile device. When parents or caregivers revoke their permission for the pupil to carry a mobile device, the school should be notified of the change.

5) Parents are reminded that in case of emergency the School's main contact number – (03)9489-1346 – remains a vital and most appropriate point of contact for ensuring a pupil is reached quickly and assisted in an appropriate way.

6) If a child is ill or distressed while under the care of the School, they must inform an appropriate member of staff. The member of staff will then determine whether it is appropriate to contact the parent/caregiver immediately to make necessary arrangements or to follow emergency procedures outlined in action plans previously provided to the school

MP3/IPOD/WIRELESS CONNECTED DEVICES

1) The School recognises that there are times when it is appropriate and useful for students to have access to a Portable Audio-visual device such as an iPod, iTouch or other MP3 player or wirelessly connected device. It is neither necessary, nor acceptable however, for these devices to be switched on or used during lesson times without the express permission of the teacher in charge.

2) Teaching staff may use portable devices to facilitate learning by disseminating lesson material via podcasting or other electronic means.

SUPPORTING DOCUMENTS

ICT Information Letter to Parents
Student User Agreement
Staff User Agreement
Harassment Policy
Privacy Policy
OH&S Policy
Insurance documentation

ACKNOWLEDGEMENTS

St John's School gratefully acknowledges the use of Melbourne Girls Grammar School's document "The Internet: Acceptable Use Policy" (February 2012).

EVALUATION

Document amended and current as at December 2018. This document is subject to regular review.