ST JOHN’S REGIONAL COLLEGE

eSMART and ACCEPTABLE USE OF ICT POLICY

This policy is to be read in conjunction with the College Mission Statement.

St John’s Regional College actively supports community access to a wide variety of information resources. We encourage community members to be able to acquire the knowledge and the skills to analyse and evaluate the use of these resources. It is expected that students, staff and parents will use ICT resources of the College in a responsible manner at all times and ensure care of all the resources.

Rationale

The College is committed to ensuring students, staff and parents have the opportunity to use ICT to educate for excellence. We are committed to ensuring that use of ICT supports staff and student learning and does not impact on the safety, wellbeing and rights of all members of the community.

Purpose

To help educate a community where excellence is promoted, we aim to recognise the importance of the use of ICT and emerging technologies and to provide the technology to staff and students to support this.

Our aim is to provide an educative environment by establishing an eSmart culture which is in keeping with the values of the College, legislative and professional obligations, and the community’s expectations. Within this context, the objectives of these guidelines are to ensure the smart, safe, responsible use of ICT within the College community.

This policy outlines the conditions applying to the use of all College ICT and emerging technologies and behaviours associated with safe, responsible and ethical use of technology. Authorised Users are required to comply with this policy and Agreement.

USER eSMART OBLIGATIONS

1. Authorised Usage and eSmart Agreement

1.1. As the College provides network access, the contents of the College ICT system, including email messages, remain the property of the College. The College has the capacity to monitor and control the system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.

1.2. All users, whether or not they make use of network facilities and communication technologies on College owned or personal ICT equipment/devices, will be issued with this Agreement. This document should be read carefully with the acknowledgment page signed and returned to the student’s homeroom teacher.

1.3. The College’s ICT, including network facilities, communication technologies, and ICT equipment/devices cannot be used until the acknowledgment page of this Agreement has been signed and returned to the student’s homeroom teacher. Signed Agreements will be filed in a secure place.

1.5. The College encourages anyone with a query about this policy or the Agreement to contact the homeroom teacher in the first instance.

2. Obligations and Requirements Regarding Appropriate Use of ICT in the College Learning Environment

2.1. While at the College, using College owned or personal ICT equipment/devices is for educational purposes only.

2.2. When using College or privately owned ICT on the College site or at any College related activity prohibited use includes, but is not limited to, any conduct that is defined as objectionable and inappropriate:

- Would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, sexism, is derogatory or threatening to another e.g. libelous, slanderous, inflammatory, threatening, harassing; has intention to deceive, impersonate or misrepresent;
- This policy extends to use of social media sites, even during out of school hours.
- Forwards confidential messages to persons to whom transmission was never authorised by the College, including persons within the College community and persons/organisations outside the College community
- Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus
- Breaches copyright
- Attempts to breach security and infrastructure that is in place to protect user safety and privacy
- Results in unauthorised external administration access to the College's electronic communication
- Propagates chain emails or uses groups or lists inappropriately to disseminate information
- Inhibits the user's ability to perform their duties productively and without unnecessary interruption,
- Interferes with the ability of others to conduct the business of the College
- Involves malicious activity resulting in deliberate damage to College ICT and/or ICT equipment devices.
- Involves the unauthorised installation and/or downloading of non-College endorsed software
- Breaches the ethos and values of the College
- Is illegal

2.3. In the event of accidental access of such material, Authorised Users must:

- Not show others
- Shut down, close or minimise the window
- Report the incident immediately to the supervising teacher.

2.4. A person who encourages, participates or otherwise knowingly acquiesces in prohibited use of College, or privately owned communication technologies, on the College site or at any College related activity, may also be found to have engaged in prohibited use.

2.5. While at the College or a College related activity, Authorised Users must not have involvement with any material which might place them at risk. This includes images or material stored on privately owned ICT equipment/devices brought onto the College site, or to any College related activity such as USB sticks.

2.6. Authorised Users must not access any database or service which charges a fee for service or access, or attempt to download, install or connect any unauthorised software or hardware onto College ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies that are available. Any Authorised Users with a query or a concern about that issue must speak with the relevant homeroom teacher, subject teacher or a member of Digital Learning or ICT Services.

3. Monitoring by the College

The College:

3.1. Reserves the right at any time to check work or data on the College's computer network, email, internet, computers and other College ICT equipment/devices, without obtaining prior consent from the Relevant Authorised User.

3.2. Reserves the right at any time to check work or data on privately owned ICT equipment on the College site or at any College related activity. The Authorised User agrees to promptly make the ICT equipment/device available to the College for purposes of any such check and to otherwise co-operate with the College in the process. Before commencing the check, the College will inform the Authorised User of the purpose of the check.

3.3. Has an electronic access monitoring system, through (among others) Meraki and Sophos, which has the capability to restrict access to certain sites and data.

3.4. Monitors traffic and material sent and received using the College's ICT infrastructures. From time to time this may be analysed and monitored to help maintain an eSmart learning environment.

3.5. From time to time conduct an internal audit of its computer network, internet access facilities, computers and other College ICT equipment/devices, or may commission an independent audit of content and usage.

4. Copyright, Licensing, and Publication

4.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Authorised Users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos, images etc.

4.2. All material submitted for internal publication must be appropriate to the College environment and copyright laws.

4.3. Any student/s found to use an ICT equipment/device to gain advantage in exams or assessments will face disciplinary actions as sanctioned by the College and other appropriate authorities e.g. VCAA.

5. Individual password logins to user accounts

5.1. If access is required to the College computer network, computers and internet access using College facilities, it is necessary to obtain a user account from the College.

5.2. Authorised Users must keep usernames and passwords confidential and not share them with anyone else. A breach of this rule could lead to users being denied access to the system.

5.3. Authorised Users must not allow another person access to any equipment/device logged in under their own user account. Material accessed on a user account is the responsibility of that user. Any inappropriate or illegal use of the computer facilities and other College ICT equipment/devices can be traced by means of this login information.

5.4. Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Guidelines and Agreement. This includes ensuring that no electronic communications could cause offence to others, harass or harm them, put the owner of the user account at potential risk, contain objectionable material or in any other way be inappropriate in the College environment.

5.5. For personal safety and having regard to Privacy laws, Authorised Users must not reveal personal information about themselves or others online. Personal information may include, but is not limited to, home addresses and telephone numbers.

6. Other Authorised User obligations

6.1. Avoid deliberate wastage of ICT related resources including bandwidth, through actions such as unnecessary printing and unnecessary internet access, uploads or downloads.

6.2. Avoid involvement in any incident in which ICT is used to send or display electronic communication, graphics, audio, video files which might cause offence to others and/or involve objectionable material.

6.3. Abide by copyright laws and obtain permission from any individual before photographing, videoing or recording them.

7. Privacy

7.1. College ICT and electronic communication should never be used to disclose personal information of another except in accordance with the College’s privacy agreement or with proper authorisation. The Privacy Act requires the College to take reasonable steps to protect the personal information that is held by the College from misuse and unauthorised access. Authorised Users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.

7.2. While after College use of communication technologies by students is the responsibility of parents, College policy requires that no student attending the College may identify, discuss, photograph or otherwise publish personal information or personal opinions about College staff, fellow students or the College. Any such behaviour that impacts negatively on the public standing of the College may result in disciplinary action. The College takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, Twitter, Myspace, YouTube, Tumblr, Snapchat, Instagram (and any further new technology).

8. Procedures for Mobile Phone and Other Electronic Device Use at College

St John's Regional College accepts that some parents provide their children with mobile phones and other personal electronic devices. However, whilst on College property and during College excursions and camps, use of mobile phones or personal electronic devices is not permitted by students unless specifically authorised by the Principal, Teacher in Charge or appropriate delegate. *Before and after school use is permitted.

Responsibility

8.1. It is the preference of the College that mobile phones and personal electronic devices are not to be brought to College

8.2. It is the responsibility of students who do bring mobile phones or personal electronic devices onto College premises to adhere to the guidelines outlined in this policy.

8.3. Students should mark their mobile phone or personal electronic device clearly with their name.

8.4. The College accepts no responsibility for replacing lost, stolen or damaged mobile phones or personal electronic devices. Their safety and security is wholly in the hands of the student.

8.5. The College accepts no responsibility for students who lose or have their mobile phones or personal electronic devices stolen while travelling to and from College.

8.6. It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.

8.7. Students must protect the privacy and dignity of individuals and security of information, to maintain the public standing of the College and compliance with State and Federal laws.

8.8. The College strongly advises that for safety reasons headphones should not be used when students are traveling to and from College, e.g. walking, riding a bike, moving on and off buses.

8.9. In accordance with College policies, any mobile phone or personal electronic device being used during the College day will be confiscated.

Parents are reminded that in cases of emergency, the College office remains a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in the appropriate way. Phone calls home to parents are to be made with a staff member.

Ratified by the College Board Date: 23rd June 2017

Appendix 1

Definitions of terms used in this Policy.

a. ‘**Authorised User’** means a person who has signed the **eSmart and Acceptable Use of ICT Agreement Form** (or has had it signed on their behalf by a parent) and is authorised by the College to use College ICT.

b. **‘eSmart’** refers to the name of the cyber safety guidelines that are followed at St John's Regional College to promote the safe, responsible and ethical use of ICT.

c. **‘ICT’** stands for ‘Information and Communication Technologies’ and includes network facilities, communication technologies, eLearning tools and ICT equipment/devices.

d. **‘Network facilities’** includes, but is not limited to, the internet access to files, iScholaris, portal access, web sites and digital resources via the College network.

e. **‘Communication technologies’** includes, but is not limited to, communication made using ICT equipment/devices such as internet, email, instant messaging, iScholaris, online discussions/surveys and mobile phone activities, iPads and related applications.

f. **‘eLearning’** refers to the use of ICT for educational purposes.

g. **‘ICT equipment/devices’** include, but are not limited to, computers (such as desktops, laptops, iPads, tablets), storage devices (such as USB and flash memory devices, CDs, DVDs, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, and any other, similar, technologies as they come into use.

h. ‘**Agreement’** refers to the eSmart Agreement which will be reviewed annually.

i. **‘College’** means St John's Regional College.

j. **‘College related activity’** includes, but is not limited to, an excursion, camp, sporting or cultural event.

k. **‘College ICT’** refers to any ICT owned or operated by the College including, but not limited to, network infrastructure, computers, cameras, iPads, tablet devices.

l. **‘Objectionable material’** includes, but is not limited to, pornography, cruelty, violence, or material of a discriminatory nature that it is likely to be detrimental to the wellbeing of students or unsuitable to a College environment.

m. **‘Unacceptable student conduct’** includes, but is not limited to, malicious or nuisance nature, invasion of privacy, harassment, bullying, cyber bullying, sexting, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, non-sanctioned gaming, impersonation/identity theft or copyright infringement.

n. **‘Educational purposes’** means activities that are directly linked to curriculum related learning.

o. **‘Personal electronic devices’** includes, but is not limited to, handheld gaming consoles (including but not limited to Nintendo DS, PSP Wii U), MP3 players (including but not limited to iPod, iPod Touch), e-readers (including but not limited to Kindle, Kobo) other internet and 3G accessible devices, and any other similar such devices as they come into use.

eSmart and Acceptable Use of ICT Agreement Form

Student Name: ____

Year Level: ______________ **Home Room:** ____________

Student agreement

I have read and understand the St John's Regional College **eSmart and Acceptable Use of ICT Agreement Form**

I understand that if the College decides that I have broken any of these rules, appropriate action will be taken which may include loss of my network and/or internet access.

While I have access to the network and internet I will:

- abide by the guidelines outlined in this policy
- use it only for curriculum related tasks
- only log on using my account, and will never share my account or password with others
- not interfere with another student's accounts or files
- not access anything illegal, dangerous or offensive.
- not reveal my full name, home address or phone numbers, or details of anyone else while accessing the internet.

Parent/Guardian agreement

I agree to my child having internet access and network privileges. I understand that ICT can provide students with valuable learning experiences. I also understand that the internet gives access to information that may be illegal, dangerous and offensive. I accept that while teachers will always exercise their duty of care, protection against exposure to harmful information should depend finally upon responsible use by students. I understand that students breaking these rules will be subject to appropriate action by the College, including loss of network and/or internet access.

I understand that the ***eSmart and Acceptable Use of ICT Policy and Agreement*** refers to both College owned and personal devices.

I understand that I must also read and sign the ***iPad Program Agreement Form*** to give permission for my child to use a school approved iPad.

Student signature: _________________________ Date: ___ / ___ / _____

Parent signature: __________________________ Date: ___ / ___ / _____

Parent name (Please print) ______________________________________