MARCELLIN COLLEGE RANDWICK

Student Acceptable Use of Technology

SCS Policy

This document incorporates the use of all digital devices (e.g. laptops, mobile phones, tablets, e-readers etc.) and online services provided by Sydney Catholic Schools (SCS). This Agreement also includes cyber safety expectations and is to be read in conjunction with the SCS Anti-Bullying Policy.

1.0 POLICY STATEMENT

1.1. Allowing students to use digital devices and providing internet services in Sydney Catholic schools is done so in order to support their educational and administrative needs. SCS acknowledges that it has a responsibility to provide safe and secure online services. These digital devices and services are educational tools and must be used in a responsible manner. This policy recognises that there are constant advances and changes in the use of technology (e.g. software, apps, information sharing, social media platforms, new devices etc.). Therefore, students must seek advice and clarification from the school as soon as possible when engaging with new or unfamiliar technology. Acceptable use is guided by the following principles:

a) Students must behave in an ethical manner when using digital devices, whether school owned or student provided BYO devices to access resources, communicate and interact with others

b) Online behaviour should at all times demonstrate a respect for the dignity of each person

c) It is never acceptable to use school or personal digital devices to harass, bully or humiliate others.

1.2. This policy informs parents and students of the school's expectations when students are using devices and services provided by SCS at school, at home, or any time they are using them for education purposes. It provides a framework for students when using their personal equipment to communicate to, or about members of the wider school community. Students whose actions contradict this policy will be subject to the school's Pastoral Care Policy and/or the Student Management: Suspension, Transfer and Exclusion Policy. This may include the withdrawal of access to services. Unacceptable material will be supplied to the NSW Police or other relevant agency (e.g. Family & Community Services etc.) by school or SCS personnel.

1.3. The school reserves the right to capture, store and review all online activity and content created or accessed via school provided services. Materials collected will remain the property of the school and SCS. School devices or BYO Devices may be confiscated or accessed where there is a reasonable belief that:

a) There has been or may be a breach of the school rules or policy

b) There may be a threat of harm to a student or others

1.4. Students will be required to cooperate with a direction from the school in providing access to the BYO devices. In an incident where this is required, parents of the students involved would be notified

1.5. Interaction with school staff on social media sites is only to occur in the context of a formal learning exercise for which parents have previously given permission.

2.0 STUDENTS PARTICIPATING IN A SCHOOL OWNED TECHNOLOGY PROGRAM

Students who use school owned devices have the following responsibilities:

2.1 To care for the laptop / device to the best of their ability

2.2 To keep the laptop / device secure and protect it from any malicious damage

2.3 Return the laptop/device (and any inclusions such as power cords and carry case) in good order

2.4 To follow all instructions and procedures set up by the school for the use of laptops/devices

2.5 To only use the Internet within the school Internet filtering system provided

2.6 To inform the teacher if the laptop / device needs charging

2.7 Log off at the end of each session to ensure that nobody else can use their account

2.8 Save all work produced and upload to their CloudShare Google Drive and not the device storage.

3.0 STUDENTS PARTICIPATING IN A BYOD PROGRAM

Students and families who are participating in a BYOD Program have the following responsibilities:

3.1 To care for and keep the device secure at all times

3.2 To acknowledge that the school cannot be held liable for any damage to or theft of BYO devices

3.3 To bring the laptop / device to school each day in readiness for use in the classroom – this includes having the battery charged and digital files effectively managed

3.4 To only use the Internet within the school proxy and filtering system provided while at school

3.5 To have all school requested apps installed on the device

3.6 To ensure any BYO device is in good working order including running the current or immediately previous operating system for the device

3.7 To install the latest antivirus and anti-malware software to the device if appropriate

3.8 To not have any "hacking" software installed on the devices

3.9 To have purchased a BYO device that meets the published device specification requirements

3.10 To not attach any BYO device to school owned equipment without permission of the school

3.11 To be aware that schools have the explicit permission to monitor and audit BYO devices brought to school by students

3.12 To be aware that BYO devices may have their serial number and Media Access Control (MAC) address recorded by the school for purposes of device identification.

4.0 CYBERSAFETY REQUIREMENTS

The Students Acceptable Use of Technology Agreement addresses the particular use of mobile technologies that has come to be referred to as 'Cyberbullying' (see 4.3 below). The school will investigate and take action where this kind of bullying occurs in school and outside of school when it causes significant harm to the relationships between students and or teachers, is criminal in nature or has the capacity to impact on relationships across the wider school community.

4.1 When using school or BYO devices to access school provided email and internet services students will:

a) Ensure that they access the internet only within the school proxy and filtering system provided

b) Ensure that communication through internet and email services is related to learning

c) Keep passwords confidential, current and private

d) Log-off at the end of each session to ensure that nobody else can use their account

e) Promptly tell their teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable

f) Seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student

g) Keep personal information including names, addresses, photographs, credit card details and telephone numbers, of themselves or others private

h) Use appropriate privacy controls for all internet and app based activities, i.e. location settings

i) Ensure that school supplied services are not used for unauthorised commercial activities unauthorised political lobbying, online gambling or any other unlawful purpose.

4.2. When using the school supplied services or BYO devices at school students will not, and will not attempt to:

a) Disable settings for virus protection, spam and internet filtering that have been applied by the school, and not attempt to evade them through use of proxy sites

b) Disable system provided apps e.g. Hapara Remote Control Extension

c) Allow others to use their personal accounts

d) Deliberately use the digital identity of another person to send messages to others or for any other purposes

e) Enter 'chat' or 'social networking' internet sites without the permission of a teacher

f) Intentionally download unauthorised software, graphics or music that are not associated with the learning activity as directed by a staff member

g) Search for or access inappropriate images, sexually explicit websites or material reasonably considered objectionable, defamatory or offensive

h) Damage or disable computers, computer systems or networks or distribute damaging files or viruses

i) Disclose or upload personal information about another person (including name, address, photos, phone numbers)

j) Take photos or video of other students, teachers or any other member of the school community without their express consent
k) Publish copyright material without proper permission or creative common attributions

4.3. When using ICT to communicate or publish digital content students will never include;
a) Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments
b) Threatening, bullying or harassing material or make unreasonable demands
c) Sexually explicit or sexually suggestive material or correspondence, as per division 15A of the Crimes Act 1900 (NSW)
d) False or defamatory information about a person or organisation
e) The school name, crest or any other identifying material without the written permission of the Principal.

Updated December 2017