Student Name: _____________________________ Class: _____________________________

STUDENT ACCEPTABLE USE of TECHNOLOGY AGREEMENT 2016

This Student Acceptable Use of Technology Agreement incorporates the use of all digital devices (e.g. laptops, mobile phones, tablets, e-readers etc.) and online services provided by the Sydney Catholic Schools Office (SCSO). This Agreement also includes cybersafety expectations and is to be read in conjunction with Sydney Catholic School’s (SCS) Anti-Bullying Policy.

The Student Acceptable Use of Technology Agreement MUST be signed by all students enrolled at a SCS. Schools are to issue the Student Acceptable Use of Technology Agreement without alteration, modification or change.

1.0 POLICY STATEMENT

1.1. Allowing students to use digital devices and providing internet services in SCSs is done so in order to support their educational and administrative needs. 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 schools' expectations when students are using devices and services whether provided by the school or BYOD, and 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. Such material is 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
   c) There may be a threat to the overall school/system security.
1.4. Students will be required to cooperate with a direction from the school in providing access to the BYOD.

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

2.0 STUDENTS PARTICIPATING IN A SCHOOL OWNED TECHNOLOGY PROGRAM

Students and their families who are participating in a school owned device program 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. 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

2.4. To return any school owned laptop / device (and any inclusions such as power cords and carry case) in good order when leaving the school.

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

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

3.8. To install the latest antivirus and antimalware software, if appropriate

3.9. To not have any “hacking” software installed on the devices

3.10. To be aware that schools have the explicit permission to monitor and audit any BYO device brought to school by students

3.11. To acknowledge that BYO devices may be accessed or ‘confiscated’ in special circumstances

3.12. To be aware that BYO devices will 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 school when it causes significant harm to the relationships between students and or teachers, or 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 requests 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 installed 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 unacceptable material
h) Damage or disable computers, computer systems or networks or distribute damaging files or viruses
i) Disclose personal information about another person (including name, address, photos, phone numbers)
j) Distribute or use information which is copyrighted without proper permission or creative common attributions
k) Take photos or video of teachers or other members of the school community without their express consent.
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

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.
STUDENT ACCEPTABLE USE of TECHNOLOGY AGREEMENT FORM 2016

Student Name: ___________________________ Class: ________________

PARENT AGREEMENT

I/we have discussed this policy with my/our child and we agree to uphold the expectations of the school in relation to the use of digital devices and services both at school and, where relevant, outside of school. We understand that a breach of this policy will incur consequences according to the school’s policies and that we will be responsible for replacing or repairing a school issued laptop / device that may be damaged, lost or stolen.

Signed __________________________________________ Date ___________ (Parent/s or Caregiver/s)

STUDENT AGREEMENT

I have read and discussed this policy with my parent / carer and I agree to be a cybersafe student and always uphold these rules both within and outside of school.

Signed __________________________________________ Date ___________
( Student - not required for children under 10 years of age)

PARENT PERMISSION TO PARTICIPATE IN E-LEARNING ACROSS ALL CURRICULUM AREAS INCLUDING THE ICT GENERAL CAPABILITIES IN THE AUSTRALIAN CURRICULUM:

Teachers may incorporate the use of online web content creation tools and sites including the CloudShare (Google Apps) Virtual Learning Environment during the course of supervised learning activity. Access to CloudShare is predicated on the provisioning of a Google Email account. Parents are requested to give permission for students to register for these sites by completing the form below. Details of the SCS policy on the use of Web 2.0 sites and learning communities can be found in the SCS Policy Staff use of Social Media in Sydney Catholic Schools.

As Parent/s / Caregiver/s I/we give permission for my child to:

- Access the internet for information relating to class work
- Publish work created by students, credited by student’s first name only
- Communicate and collaborate with others within the school, and organisations outside of the school, with approval from teachers
- Use a variety of websites, including registration and personal usernames and passwords, for educational purposes including CloudShare (Google Apps for Education).

Please note that the students will access the internet with a username and password. Please indicate your permission by ticking the appropriate boxes above. The preferred option would be for all boxes to be ticked so that students are able to make optimum use of the technology and actively participate in all lessons.

Signed __________________________________________ Date ___________
(Parent/s or Caregiver/s)

Student’s name __________________________________________ Class __________
(Please print student’s name)