



STUDENT ACCEPTABLE USE AGREEMENT FORM 2014

RE: digital devices (e.g. laptops, mobile phones, iPads etc.) and services – including cybersafety expectations. To be read in conjunction with the CEO Sydney's Anti-Bullying Policy

POLICY STATEMENT

The use of digital devices and points of access to email and Internet services in Catholic Education Office (CEO) Sydney schools is provided to students 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 (including for e.g. software, apps, information sharing, social media platforms, new devices etc and this list is not exhaustive). 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.

- Students must behave in an ethical manner when using digital devices, whether school owned or student provided devices (Bring Your Own Devices "BYOD") to access resources, communicate and interact with others.
- Online behaviour should at all times demonstrate a Christ-centred respect for the dignity of each person.
- It is never acceptable to use digital devices to harass, bully or humiliate others.

This Policy informs parents and students of our school's expectations when students are using the devices and services provided 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 (for e.g. Family & Community Services etc) at the discretion of school or CEO Sydney personnel.

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 the CEO. School devices or BYOD may be taken or accessed where there is a reasonable belief that:

- There has been or may be a breach of the school rules or policy
- There may be a threat of harm to a student or others or system security.

Students will cooperate with a direction from the school in providing access to the BYOD.

Interaction with school staff on social media sites is only to occur in the context of a formal learning exercise which parents have been alerted to formally in advance.

STUDENTS USING SCHOOL OWNED TECHNOLOGY

Students and their families who use a school owned device have the following responsibilities:

- To care for the laptop / device to the best of their ability.
- To keep the laptop / device secure and protect it from any malicious damage.
- 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.

- **To replace or repair any damaged, lost or stolen laptop / device at their own cost.**
- To return the school owned laptop / device (and any inclusions such as power cords and carry case) in good order when leaving the school.

CYBERSAFETY REQUIREMENTS

This policy addresses the particular use of these technologies that has come to be referred to as '**Cyberbullying**' (See No 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, or is criminal in nature or has the capacity to impact on relationships across the wider school community.

1. When using school and personal devices and services **students will**:
 - ensure that they access the Internet only within the school proxy and filtering system provided.
 - ensure that communication through Internet and email services is related to learning.
 - keep passwords confidential, current and private.
 - log off at the end of each session to ensure that nobody else can use their account.
 - 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.
 - seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
 - keep personal information including names, addresses, photographs, credit card details and telephone numbers, of themselves or others, private.
 - Use appropriate privacy controls for all internet and app based activities. i.e. location settings
 - ensure that school services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
2. When using the school services or personal mobile phones (or similar personal equipment) **students will not, and will not attempt to:**
 - 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.
 - disable system installed apps eg. Hapara Remote Control Extension
 - allow others to use their personal accounts.
 - deliberately use the digital identity of another person to send messages to others or for any other purposes.
 - enter 'chat' or 'social networking' internet sites without the permission of a teacher.
 - intentionally download unauthorised software, graphics or music that are not associated with the learning activity as directed by a staff member.
 - damage or disable computers, computer systems or networks or distribute damaging files or viruses.
 - disclose personal information about another person (including name, address, photos, phone numbers)
 - distribute or use information which is copyrighted without proper permission.
 - take photos or video of members of the school community without their consent.
3. When using ICT to communicate or publish digital content students will **never** include;
 - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
 - threatening, bullying or harassing material or make unreasonable demands.
 - sexually explicit or sexually suggestive material or correspondence.
 - false or defamatory information about a person or organisation.
 - the school name or crest without the written permission of the Principal.

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 Pastoral Care Policy 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 ELEARNING ACROSS ALL CURRICULUM AREAS INCLUDING THE ICT GENERAL CAPABILITIES IN THE AUSTRALIAN CURRICULUM:

Teachers may incorporate the use of online web 2.0 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 CEO policy on the use of Web 2.0 sites and learning communities can be found in the CEO 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.
- To publish work created by students, credited by students' first name only.
- Communicate and collaborate with others within the school, and organisations outside of the school, with approval from teachers.
- Use of a variety of websites, including registration and the use of personal usernames and passwords, for educational purposes including CloudShare (Google Apps for Education).

Please note that the students will access the Internet using 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)