Catholic Education
Diocese of Cairns
Learning with Faith and Vision

NAME OF SCHOOL: St Stephen's Catholic College

SUBURB: Mareeba

ACCEPTABLE USE OF COMPUTER AND INTERNET RESOURCES - SECONDARY

Computer and internet resources are of critical importance to schools in facilitating and supporting learning and teaching. **Technology resources are provided to students for educational purposes only and must be used in a responsible manner.**

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 always 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.
- All devices must be enrolled in the CES Mobile Device Manager (MDM) to access network and online services.

This agreement informs parents and students of our school's expectations when students are using the devices and services provided, whether 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 will be subject to the school's Behaviour Management processes. This may include the withdrawal of access to services. Unacceptable material will be supplied to the Police or other relevant agency at the discretion of the school or Catholic Education Services (CES) Cairns.

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 CES Cairns. 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.
- There may be a threat of harm to a student or others or system security.

Students will cooperate with a directive 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 activity**.**

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.

Secondary cyber safety requirements

This section outlines ethical and safe use of ICT (Information and Communications Technology) and addresses the 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.
    - 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.
    - Ensure copyright and intellectual property requirements are followed.
    - Only access applications and sites as per their terms of use and age requirements (e.g. 13+, 17+).
    - Seek advice and clarification from the school as soon as possible when engaging with new or unfamiliar technology.

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 e.g. Hapara, Company Portal.
    - 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.
    - Participate in 'social networking' 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.

4. If inappropriate material is accidentally accessed students **will:**

1. Not show others
2. Turn off the screen or minimise the window and
3. Report the incident to a teacher immediately.

Agreements

eLEARNING ACROSS THE CURRICULUM

Teachers may incorporate the use of online web tools and sites including cloud computing as part of supervised learning activities. Access to cloud computing is predicated on the provisioning of a Google Email account. The use of Google and Microsoft 365 Apps is supported by a signed agreement between Catholic Education and these providers, acknowledging their commitment in ensuring a safe and secure environment for students to use.

ICT Supported Education Activities may include:

- Accessing the internet for information relating to class work.
- Publishing work created by students, credited by students' first name only.
- Communication and collaboration 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 cloud computing (e.g. Google Workspace for Education).

PARENT AGREEMENT

I/we have discussed this agreement 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 Behaviour Management Policy and that we will be responsible for replacing or repairing a school issued laptop/device that may be damaged, lost or stolen.

NAME: _____ **DATE:** _____

SIGNATURE: _____ 

(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.

NAME: _____ **HOME GROUP/PC CLASS:** _____

SIGNATURE: _____ 

DATE: _____