



# Digital Technology Acceptable Use Policy

---

## Policy Statement

SCCC values the safety and privacy of all students when accessing and using digital technology. The SCCC Digital Technology Acceptable Use Policy outlines the procedures and expectations for students using technology at the College.

## Rationale

The safety of students when accessing digital technology is of critical importance with the increased access to digital resources in the College. The Digital Technology Acceptable Use Policy is designed to protect the safety of all users and associated hardware and software.

## Scope

This policy will be adhered to by students and monitored by all staff in the classroom and while in the playground. Upon signing this document parents are expected to discuss acceptable use with their son/daughter and support the College in the safe and respectful use of Digital Resources as outlined.

## Principles

By accessing and using the Digital Technology provided by SCCC, you agree to abide by SCCC Digital Technology – Acceptable Use Guidelines.

Access to computer resources and all privately owned digital technology is governed by this Acceptable Use Policy.

### a. Personal Technology

- a. Mobile phones are not to be used or accessed in class;
- b. Google Glass and the Apple Watch are not permitted at school.

### b. Ethical, legal and responsible use of digital technology

SCCC requires all users of its digital technology to do so in an ethical, legal, responsible manner in accordance with the values of the College.

- a. Student use of digital resources is subject to the full range of laws that apply to the internet, communications and to the use of computers, and related College policies. This includes, but is not limited to, copyright, intellectual property, breach of confidence, defamation, privacy, bullying/harassment, vilification and anti-discrimination legislation, the creation of contractual obligations, and other civil and criminal laws.
- b. **SCCC** digital resources must not be used for unauthorised commercial activities or unauthorised personal gain. Actions performed using **SCCC** digital resources must comply with the terms of any licence agreed to for the use of software programs and other online resources.

- c. When using personal or College owned digital technology it is unacceptable for students to:
  - Associate SCCC with sites that compromise the good name of the College.
  - Using the College name in contexts and behaviours that are contrary to our College values and ethos.
  - Post photographs on the internet that associate SCCC or its students with unacceptable behaviour.

### **c. Copyright and Intellectual Property Rights**

- a. Users must not, through the use of SCCC digital resources, copy, download, store or transmit material which infringes copyright or the intellectual property rights of others without appropriate approval. Such material includes music files, movies, videos or any other form of media.
- b. Students should be aware that actions performed using SCCC digital resources, regardless of any disclaimers that might be made, ultimately reflect on our educational institution and community as a whole.

### **d. Use of the College wireless network and internet access**

- a. The use of the College wireless network and all associated infrastructure are available for educational use with student Laptop computers or other approved College technology.
- b. The internet is only to be accessed through the College wireless network while at school. The use of personal hotspot devices is not permitted.
- c. The downloading of large files is monitored and not permitted due to bandwidth limitations.
- d. Students are not permitted to override College filtering systems.
- e. Specific network settings are not to be removed or altered as this could affect the Laptop computer's ability to connect to the College wireless network.

### **e. Security and Privacy**

- a. Users are issued with unique usernames and passwords, which should be kept strictly confidential at all times.
- b. Users must protect systems, information and accounts by:
  - Choosing a secure password which is changed regularly;
  - Using access to digital resources only as authorised;
  - Respecting the privacy and confidentiality of information that they may come across through access to digital resources;
  - Only downloading, installing or using authorised software;
  - Reporting any breach or prospective breach of network security to the appropriate technical personnel or the ICT Services Help Desk;
- c. Unacceptable conduct by users which could result in a breach of security or privacy includes:
  - Disclosing your username and password details to another person;
  - Disclosing private or confidential information to unauthorised persons;
  - Gaining unauthorised access to any systems by any means;
  - Using SCCC digital resources to attack or compromise another system or network;
  - Downloading, installing or using unauthorised or illegal software and data;
  - Deliberately installing computer viruses or other malicious programs;
  - Using devices like mobile phones linked to the laptop to avoid the filtering and security system of the College;
  - Accessing or intercepting electronic communications without permission.
- d. Users should not, as a general rule, display personal information about themselves in a way that is publicly available.

- e. Users must be aware that the operation and maintenance of digital resources within the College are monitored; complete confidentiality and privacy cannot be guaranteed. **SCCC** may also be required to inspect digital resources or provide copies of electronic communications where required to by law, or where the possible misuse of digital resources is suspected.

**f. Breaches of Acceptable Use Guidelines**

- a. A breach of the Acceptable Use Policy will be taken seriously and may result in disciplinary action being taken. Examples of possible consequences include;
  - Loss or restriction of access to digital technology
  - Mobile phone confiscation
  - Formal disciplinary action for breach of the Student Behaviour Code
  - Suspension

Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.

**Policy Update**

*This policy will be updated as necessary. All attempts will be made to adhere to the above policy, but particular circumstances (such as technological advancements) may require the Principal to depart from the stated policy.*



.....

## Southern Cross Catholic College Digital Technology Access Consent Form

**Student Acceptance**

I confirm that I have read and agree to abide by the *SCCC Digital Technology Acceptable Use Policy* and all other relevant laws and restrictions associated with digital resources. In the event of any breach I acknowledge that appropriate disciplinary action may result.

**NAME:** \_\_\_\_\_

**PC CLASS:** \_\_\_\_\_

**SIGNATURE:** \_\_\_\_\_

**DATE:** \_\_\_\_\_

**Parent/Guardian Consent**

I confirm that I have read the *SCCC Digital Technology Acceptable Use Policy*. In the event of any breach I acknowledge that appropriate disciplinary action may result.

I acknowledge that some material available on the internet may be objectionable and that in addition to the *Digital Technology Acceptable Use Policy* statement there are other laws and restrictions associated with digital technology. I have discussed appropriate restrictions for the student when accessing or sharing information or material over the internet.

As the parent/legal guardian of the student named above, I grant permission for them to access digital technology as part of the curriculum at the College.

**NAME:** \_\_\_\_\_

**DATE:** \_\_\_\_\_

**PARENT SIGNATURE:** \_\_\_\_\_