



## Information Communication Technologies Acceptable Use Policy

### 1 Context

- 1.1 Cabra acknowledges that ICT, the internet and social media can be powerful tools for use in our educational search for truth, beauty and the good in the world. As such, we seek to empower students to use these tools in a manner befitting the College's Catholic ethos and Dominican ideals of praising, blessing and teaching.
- 1.2 Cabra holds the view that children and young people grow to their full potential when they are provided with a spiritual, emotional and physical environment that is enriching and safe.
- 1.3 Cabra recognises and teaches its students that all internet users have a digital or online reputation.
- 1.4 Cabra expects technology to be used in a safe, responsible, respectful, and ethical manner at all times.

### 2 Policy Statement

- 2.1 Cabra's ICT Facilities are used for both administrative and educational purposes. These resources enable greater communication between staff, students, and parents/caregivers, creating digital learning environments where students can motivate themselves and each other to become independent, lifelong learners.
- 2.2 Learning, communication, and collaboration are enhanced through access to the ICT Facilities.
- 2.3 At all times use of ICT must be in keeping with legal requirements, the Catholic Dominican ethos, and policies of Cabra.
- 2.4 The principles set out in this policy cover the acceptable use of Cabra's ICT.

### 3 Definitions

**Employees** has its ordinary meaning and includes volunteers engaged by the College.

**ICT Facilities** means the College ICT, including the network, hardware, cloud-based resources, data networks, infrastructure (such as wireless access points), computers, hardware (such as monitors and keyboards), printers, and all means of electronic communication provided by the College.

**Information Communication Technology (ICT)** includes any facilities used to compute, communicate and to store information electronically. This may include, and is not limited to, desktop, laptop, and tablet computers, computer servers, personal mobile devices, electronic storage devices, network and telecommunications equipment and associated software.

**Personal ICT Device** means a device that is not owned by Cabra, but which is used to access the ICT Facilities.

**Online/Remote Learning** means any lesson or meeting which replaces face-to-face contact and takes place across the internet.



## 4 Scope

- 4.1 This Policy applies to students, Employees and parents and caregivers.
- 4.2 This Policy governs the use of the ICT Facilities, regardless of whether the ICT Facilities are used on-site or off-site, or inside or outside of normal working or school hours. To avoid doubt, this includes online learning and remote access to ICT Facilities.
- 4.3 This Policy governs the use of Personal ICT Devices used in conjunction with the ICT Facilities.

## 5 General Principles

- 5.1 All of the College's ICT Facilities are to be:
  - (a) used in accordance with their intended use;
  - (b) handled in a respectful manner (to the extent ICT Facilities are hardware); and
  - (c) used in an ethical, professional, and lawful manner.
- 5.2 Anyone with access to ICT Facilities must:
  - (a) maintain a secure username and password, and ensure that they do not provide their password to anyone else; and
  - (b) ensure that they do not permit or facilitate unauthorised use of ICT Facilities by anyone.
- 5.3 Students and Employees must not use ICT to:
  - (a) bully or harass another member of the community, in breach of the Bullying and Harassment Prevention Policy or the Cabra Working Together Principles;
  - (b) gain unauthorised access to anyone else's account or user information
  - (c) attempt to defeat any security controls (i.e., through using a virtual private network ("VPN") or proxy servers);
  - (d) to use another person's email account or other means of communication to send any communication in that other person's name (unless specifically authorised by that person);
  - (e) to spam, spoof or mass mail or to send or receive chain mail;
  - (f) to take photos or video of members of the school community without their consent;
  - (g) to send, receive, or store obscene, offensive or pornographic material;
  - (h) to infringe the copyright or other intellectual property rights of another person;
  - (i) to injure the reputation of the College and or the Church in a manner that may cause embarrassment to the employer or the Church; or
  - (j) to perform any other unlawful or inappropriate act.
  - (k) Forward or send links to online lessons or meetings to people outside the Cabra Community which enables unauthorised access to the College.
- 5.4 People to whom this policy applies must never use a VPN.



- 5.5 Any document transmitted or stored on the College's computer network may be accessed by the Principal or the Principal's delegate. As such, students and Employees should not expect that any information or document transmitted or stored via the ICT Facilities is private.
- 5.6 People to whom this policy applies should be aware that they may be liable for what is communicated (whether by written word, spoken word, image, or other means) in any form of ICT. To avoid doubt, communication made on a Personal ICT Device about a member of the Cabra community is governed by this policy and other applicable policies (such as the Bullying and Harassment Prevention Policy and Grievance Policy).
- 5.7 Students and Employees are responsible for:
- (a) the safekeeping of their Personal ICT Devices or ICT devices provided to them by Cabra;
  - (b) ensuring that other people do not access any confidential information contained on the device, and
- where an ICT device provided by Cabra has become damaged or subjected to unauthorised access, the student or Employee must notify Cabra ICT staff or a Deputy Principal as soon as practicable.

### Student-specific principles

- 5.8 All students have individual user accounts that provide access to the ICT Facilities, including email and Learning Management Systems.
- 5.9 The internet is in a perpetual state of evolution and as such the College claims no control over the content or subject matter of the information available via the internet and email but aims to monitor and promote responsible use of this valuable medium.
- 5.10 Students must:
- (a) ensure their Personal ICT Device is fully charged before arriving at school;
  - (b) use the ICT Facilities for school-related activities and research;
  - (c) treat ICT Facilities carefully and with respect, and alert teachers of any problems.

### Cabra's educative approach

- 5.11 Cabra acknowledges its role in educating its students about ICT, with a particular focus on responsible, safe and ethical usage in order to become responsible digital citizens.
- 5.12 Cabra aims to provide and maintain a cyber-safe culture that is in keeping with our Catholic ethos.
- 5.13 A strict one-size-fits-all approach to ICT will not adequately cater to the needs of everyone. Use of Personal ICT Devices supports students in their diverse learning styles.

## 6 Breaches

- 6.1 Parties to whom this policy applies should report any breach of this Policy (whether accidental or intentional) or any other suspicious online activity as soon as practicable.
- 6.2 Behaviour that breaches this policy will be taken seriously and may result in disciplinary action being taken.

- 6.3 Depending on the infringement, serious consequences for students such as a sanction, suspension, expulsion or ban on using any of the ICT Facilities may occur.
- 6.4 In the event that a staff member is found to have breached this Policy, consequences may include:
- (a) verbal counselling or warning;
  - (b) written counselling or warning;
  - (c) formal final warning; or
  - (d) dismissal,
- as well as limitation or suspension of some or all of the staff's right to use the College's ICT Facilities. Any investigation will be carried out in accordance with the "Procedures for Dealing with Allegations of Misconduct" (SACCS).
- 6.5 Cases of serious, deliberate and/or criminal breach will be referred to external authorities (including SAPOL or the Australian Federal Police) and may result in civil or criminal proceedings.

## 7 Related Documents and References

- Cabra Dominican College Bullying and Harassment Prevention Policy
- Cabra Dominican College Data Breach Policy and Procedure
- Cabra Dominican College Developing Personal Responsibility Policy
- Cabra Dominican College Principles for Working Together
- Cabra Dominican College Privacy Policy
- Cabra Dominican College Safeguarding Children Policy
- Cabra Dominican College Staff Handbook
- Cabra Dominican College Student Handbook
- SACCS Information Security Policy and Guidelines (2020)
- SACCS Managing Allegations of Misconduct Guidelines (2019)

## 8 Revision Record

Document Title	ICT Acceptable Use Policy						
Document Type	Policy						
Document Date	November 2021						
Process Owner	Deputy Principal: People, Culture and Operations						
Contact	Jarrad McCabe ( <a href="mailto:jmccabe@cabra.catholic.edu.au">jmccabe@cabra.catholic.edu.au</a> )						
Approval Authority	Executive Leadership Team						
Review Date	November 2024						
Policy Distribution	Website	✓	MS Teams	✓	SEQTA	✓	BoardTrac
Revision History	<b>Edition Number</b>	<b>Date</b>	<b>Description of change</b>				
	1.0	2018					
	2.0	2021	Updated to reflect new SACCS Policies Revision to new style guide				