Responsible Use of Technology Policy

1. Purpose and Objectives

As Canterbury College is an independent school, based on Christian values, this policy aims to provide direction and appropriate boundaries in using technologies responsibly. It aims to support staff and students to meet the high standards expected within our Vision, Values and Code of Conduct, as well as state or federal legislation. The College is protective of its image and "brand" and will promote and protect itself to maintain its fine reputation.

Canterbury College provides resources in and access to technologies to staff and students, which are required to be used ethically, safely, respectfully, and responsibly, with a view to enhancing educational experiences and educational outcomes. It is expected that the protection of the privacy and security of Canterbury College employees, students, parents of students, partners, branding, suppliers, and property will apply to all students and employees. It is expected that all students and employees will comply with applicable laws and legislation.

Providing users with access to a vast amount of unfiltered information necessarily raises concerns that users will be exposed to ideas or material that may be unhealthy, or at the very least, non-educational or relevant to our core purpose. Therefore, it is highly appropriate for educational systems and employers to exert control over the use of the services they provide.

2. Definitions, Terms, Acronyms

Canterbury College	Canterbury College Ltd or any controlled entities of Canterbury College Ltd.
Social Media	A group of web-based applications that enable the creation and exchange of user-generated content. Social Media occurs in a variety of formats including chat rooms, web blogs, social blogs, wikis, microblogging, internet for a, podcasts, pictures, video and rating and social bookmarking. Examples of Social Media include but are not limited to Facebook, LinkedIn, MySpace, YouTube, Flickr, Vimeo, Instagram, Tik Tok, Snapchat, Discord and Twitter.
Users	Includes staff, students and by default parents/guardians of enrolled students as accepted under the Enrolment Contract.
Mobile Phone	Mobile phones are any telephone with access to a cellular radio system so it can be used over a wide area, without a physical connection to a network.
SIM-enabled Device	A SIM-enabled device is any device that uses a SIM card (subscriber identity module) to access cellular telephone services or data. This includes but not limited to mobile phones, smartwatches, iPads, or other tablet devices.
Electronic Device	Other electronic devices include, but not limited to, smartwatches, iPads, iPods, other tablet devices, digital cameras, or other wearable technologies.

3. Policy Scope/Coverage

This policy applies to all students and employees of Canterbury College.

4. Policy statement

4.1 Users must not access material where content would be inconsistent with the Vision and Values of Canterbury College, nor must use of services be for purposes contrary to the law or Canterbury College Code of Conduct.

4.2 Users shall not access any objectionable or offensive material, material contrary to the law or material inappropriate to an educational or work environment. Types of inappropriate use and websites appears in the Appendices.

4.3 Users shall not post or forward defamatory, inaccurate, personal, sensitive, abusive, obscene, profane, sexually orientated, threatening, offensive or illegal material.

4.4 Email messages or attachments that contain, or are reasonably suspected to contain, offensive material must not be opened or sent.

4.5 Users must not personally subscribe to any External Mailing lists without the written approval of the Principal or Head of Sub-School.

4.6 The network administrator may close an account at any time or as requested (e.g., by parent, Principal, Head of Sub-School).

4.7 Users who suspect or know of inappropriate use must report such use to the Principal or Head of Sub-School.

4.8 At the discretion of the Principal or Head of Sub-School, any person identified as a security risk may be denied access to Canterbury College technology services.

4.9 Users should be aware that breach of this policy might also lead to external action being taken against them by a third party (e.g., for breach of Anti-Discrimination laws or defamation).

4.10 Good systems administration includes regular backups and the monitoring of logs reflecting all use of technology systems. Normal systems administration may have the effect of collecting information provided by the user, including email messages, both active and deleted, as well as internet sites visited. The right is reserved to monitor user activity to ensure adherence to the principles of this document and then to act as deemed appropriate. Individualised searches will be conducted if there is a reasonable suspicion that a user has violated the law or school rules.

4.11 All users are directed not to publish identifying information about children or photographs of children on the internet without consent of the Principal.

4.12 The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Commonwealth) applies to private educational institutions and establishes thirteen (13) Australian Privacy Principles and must be complied with by Canterbury College.

4.13 All attempts should be made to keep information secure. A common means of gaining illegal access to electronic information is to break a legitimate user's password. Users should select passwords that are not easy to guess or to find out by a password-breaking program. Passwords need to be changed regularly.

5. Guidelines/Procedure/Process

5.1 Procedure – Students

5.1.1 Those using technologies need to do so with the intent to meet the College's expectations.

5.1.2 Students will be instructed in responsible use of technologies by teachers but are also expected to inform themselves of correct procedures and possible consequences.

5.1.3 The 'Acceptable Use of Mobile Phones, SIM-enabled and Electronic Devices Policy' compliments this policy and covers all matters related to such devices.

5.1.4 The College will endeavour to provide resources and appropriate levels of training to students in the responsible use of technologies.

5.1.5 The College's expectations also apply to usage of the College's resources outside of hours or usage off site.

5.1.6 Users of the College's technology resources are expected to keep secure the equipment used, access to information and personal access passwords.

5.1.7 Users are expected to obey copyright laws and the intellectual property of third parties.

5.1.8 Person(s) found to misuse, intend to damage, or actually damage the College's resources or another party's files, are liable to prosecution and/or other school level consequences in line with the 'Student Behaviour Policy'.

5.1.9 The use of College or other resources to communicate in a manner, which includes images, or content that the College deems offensive could lead to prosecution and/or other school level consequences in line with the 'Student Behaviour Policy'. These include but are not limited to racist, vulgar, derogatory, obscene, or harassing communications. Communication pathways include but are not limited to inappropriate or illegal websites, social networking sites, email, and SMS messaging.

5.1.10 The use of College or other devices/resources in acquiring, storing, communicating, "posting" or "uploading" content which has a linkage to Canterbury College, by way of naming or images, requires College approval. Images or content, which are deemed offensive/inappropriate by the College, could lead to prosecution and/or other school level consequences in line with the 'Student Behaviour Policy'.

5.1.11 Users are to ensure that digital memory devices brought to the College or used on its network will not damage College resources.

5.1.12 The College's technology system is neither private nor secret. Usage of the College's resources is monitored and can have information intercepted. In this light, the College reserves the right to examine its computer network to ensure compliance with the terms of this policy.

5.1.13 Matters relating to the use of technology in all forms of academic misconduct, including but not limited to cheating, plagiarism and non-submission are dealt with by the terms of the 'Assessment Policy'.

5.1.14 The College will be supportive in assisting parents to educate their students in cyber safety and responsible use of technologies as they apply to the College's programs and equally expects parents to support this policy and its procedures, to respect and value the reputations of individuals and the College.

5.2 Procedure – Staff

5.2.1 Those using technologies need to do so with the intent to meet the College's expectations.

5.2.2 Staff are expected to inform themselves of correct procedures and possible consequences, as a responsible employee.

5.2.3 The College will endeavour to provide resources and appropriate levels of training to staff in the responsible use of technologies. Staff are expected to undertake additional professional development to enhance their proficiency above the entry level provided by the College.

5.2.4 The College's expectations apply to usage of the College's and personal resources outside of hours or usage off site.

5.2.5 Users of the College's technology resources are expected to keep secure the equipment used access to information and personal access passwords. Securing College equipment involves locking access to staff areas and placing equipment in secure, out of sight locations after hours.

5.2.6 Users are expected to obey copyright laws and the intellectual property rights of third parties.

5.2.7 Staff using mobile or fixed equipment in their teaching lessons are to ensure equipment is checked prior to and at the conclusion of a lesson. Any matters requiring attention, including repairs are to be communicated with the IT team as a matter of urgency.

5.2.8 Staff are responsible for monitoring student usage of software and hardware in each of their lessons. Where appropriate, they should outline and explain the College's expectations to students in relation to responsible use of technologies.

5.2.9 Person(s) found to misuse, intend to damage, or damage the College's resources or another party's files, are liable to prosecution and/or other school level consequences, including suspension and termination.

5.2.10 The use of College or personal resources to communicate in a manner that includes images or content that the College deems offensive or inappropriate could lead to prosecution and/or other school level consequences, including suspension and termination. These include but are not limited to racist, vulgar, derogatory, obscene, or harassing communications. Communication pathways include but are not limited to inappropriate or illegal websites, social networking sites, email, and SMS messaging.

5.2.11 The use of College or personal devices/resources in communications, "posting" or "uploading" involving linkage to Canterbury College, by way of naming or images, requires College approval. Images or content, which is deemed offensive/inappropriate by the College, could lead to prosecution and/or other school level consequences, including suspension and termination.

5.2.12 The use of devices, without College permission, to take images for storage or transmission involving the use of the College's name or images that enable linkage to the College could result in prosecution and/or other school level consequences, including suspension and termination.

5.2.13 Staff are not to communicate with students via social networking or methods that could be interpreted as social contact and so unprofessional conduct, in accordance with the Teacher Professional Standards, Code of Conduct for Anglican Schools and Education and Care Services and the 'Staff Social Media Policy'.

5.2.14 Staff are expected to conduct themselves professionally when using technology, such as social networking sites outside of school, especially if their conduct has implications for the College.

5.2.15 Staff are to ensure that digital memory devices brought to the College or used on its network will not damage College resources.

5.2.16 Personal devices such as phones are brought to school or school events at the owner's risk. The College takes no responsibility for care or security.

5.2.17 Staff who become aware of behaviours contrary to this College policy are to report the matter to an appropriate member of the Executive Team (Head of Sub-School, Director of Business and Finance or the Principal).

5.2.18 Staff communication via email, in relation to academic or pastoral matters with parents/guardians or students, should have an appropriate manager copied in the email.

5.2.19 The College's technology system is neither private nor secret. Usage of the College's resources is monitored and can have information intercepted. In this light, the College reserves the right to examine its computer network to ensure compliance.

5.2.20 Phones should not be used during lessons.

5.2.21 Staff who suspect inappropriate content is being accessed or stored in a manner linked to the College should report their concern to an appropriate member of the Executive Team (Head of Sub-School, Director of Business and Finance or the Principal) as a matter of urgency. Staff who may be requested to locate or identify the inappropriate content, have the right to request another staff member investigate the nature of the concern.

5.2.22 Staff should be aware that whether on or off duty, a College employee's conduct (both online and offline) will reflect on Canterbury College and all employees must protect the reputation of the College.

5.2.23 Breaches of any College Policy or Professional Standards may result in managerial action including dismissal and/or criminal reporting and/or civil sanctions.

5.2.24 If a College employee becomes aware of a social media site or posting that;

- is illegal, or alludes to criminal behaviour in association with Canterbury College in any way,
- defames Canterbury College, or presents Canterbury College in a negative manner,
- breaches this Policy or its stated purpose herein, or related Policies pertaining to Child Protection, or Professional Standards.

The College Employee must immediately report it to an appropriate member of the Executive Team.

6. Roles and Responsibilities

Students

- All students are expected to use the College's technologies and those owned or operated by other parties in a manner, which enhances the learning experiences offered and promotes the College's values.
- As members of the College community, parents and guardians are expected to conduct themselves in a manner, which reflects the College's values, when using technologies which have a linkage in use or content related to Canterbury College.
- Person(s) who undertake unauthorised use of technologies provided at the College will be responsible for any financial obligations, which arise from such unauthorised usage.

Staff

- All staff are expected to use the College's technologies and those owned or operated by other parties in a manner, which enhances the learning experiences offered and promotes the College's Values.
- Person(s) who undertake unauthorised use of technologies provided at the College will be responsible for any financial obligations, which arise from such unauthorised usage.
- Staff are expected to regularly ensure that students are informed on the correct and safe use of technologies and to monitor student usage.

7. Review

This policy and its associated procedures, quick reference guides and protocols will be reviewed in accordance with the College's policy review processes. Canterbury College, however, reserves the right to review this policy at any time.

8. Appendices

8.1 Inappropriate Use

The use of the intranet, internet and email must not be used to:

8.1.1 Infringe the copyright or other intellectual property rights of third parties, for example, staff should not download and use work without the express permission of the owner.

8.1.2 Download software, unless appropriate authorisation and compliance with licensing requirements and established policies to check all such software for computer viruses is followed.

8.1.3 Adult sites, images or statements or other material obtained from

inappropriate internet sites.

8.1.4 Access inappropriate internet sites (see below).

8.1.5 Disrupt communication and information devices through such means as mass emailing or transmitting files which place an unnecessary burden on departmental resources.

8.1.6 Download, distribute, store, or display offensive or pornographic graphics.

8.1.7 Access material that is discriminatory or could cause offense to others, for example, offensive material based on gender, ethnicity or religious or political beliefs.

8.1.8 Download unreasonable amounts of material for non-work related or non-educational use.

8.1.9 Download information for the purpose of providing it to external organisations or the public without authorisation.

8.1.10 Distribute chain letters.

8.1.11 Distribute defamatory, obscene, offensive, or harassing messages.

8.1.12 Distribute confidential information without authority.

8.1.13 Distribute messages that disclose personal/sensitive information without authorisation.

8.1.14 Distribute private information about other people.

8.1.15 Distribute messages anonymously, using a false identity or using another person's email account.

8.1.16 Engage in any illegal or wrongful activity.

8.1.17 Download/supply to others inappropriate site addresses; and

8.1.18 Knowingly engaging in any activity which may compromise the security of the local area network, intranet, or external network.

8.2 Inappropriate Internet Sites

Inappropriate sites include, but are not limited to, sites that:

8.2.1 Are illegal.

8.2.2 Are pornographic or contain inappropriate or obscene sexual material.

8.2.3 Advocate hate/violence.

8.2.4 Contain discriminatory material, e.g., based on gender, race, religious or political beliefs, and offer inappropriate games or software.

Version Number:	v1.02023
Policy Library:	Business/Finance
Responsible Officer	Director of Business and Finance
Approval Authority:	College Executive
Last Approval Date:	January 2023
Review Date:	January 2024
Related Policies/Procedures:	Acceptable Use of Mobile Phone Policy Assessment Policy Behaviour Policy Code of Conduct for Anglican Schools and Education and Care Services Staff Social Media Policy Teacher Professional Standards
Acknowledgements:	Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth)