

Acceptable Use of Technology Policy

Contents

1. Purpose and Objectives`	2
2. Definitions, Terms, Acronyms	2
3. Policy Scope/Coverage	3
4. Policy statement	3
5. Data Protection and Privacy	4
6. Intellectual Property and Data Ownership.....	5
8. Guidelines/Procedure/Process	5
9. Review	6

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 employees 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 exemplar reputation.

Canterbury College employees and students with access to technology resources. This privilege is provided on the understanding that it will be used ethically, safely, respectfully and responsibly, and to enhance 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

Canterbury College exerts control over the services provided to employees and students to ensure that:

- Privacy is maintained;
- Security measures are adhered to;
- Only acceptable, age-appropriate information is available as deemed relevant to our core purpose.
- Access to information throughout the system is managed and authorised in terms of requirements.

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, podcasts, pictures, video and rating and social bookmarking. Examples of social media include but are not limited to Facebook, LinkedIn, TikTok, Snapchat, YouTube, Flickr, Vimeo, Instagram and Twitter.
Users	Includes employee, students and their parents/guardians s as accepted under the Enrolment Contract.
Technologies	Includes all College-owned, leased, managed or authorised hardware, and software,
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether recorded in a material form or not, as defined under the Privacy Act 1988 (Cth). Examples include a person’s name, address, contact details, date of birth, and enrolment or employment records.

Personally Identifiable Information (PII)	Any data that could be used, on its own or combined with other information, to identify a specific individual. This includes information such as names, student or staff identification numbers, photographs, email addresses, and financial or health details.
Sensitive Information	A subset of Personal Information that requires a higher level of protection, including information about an individual's health, racial or ethnic origin, religious beliefs, or other categories defined under the <i>Privacy Act 1988 (Cth)</i> .
Data Breach	An incident in which Personal Information held by the College is subject to unauthorised access, unauthorised disclosure, loss or misuse. A data breach may be accidental or deliberate.
Data Protection	The practices, safeguards and legal obligations put in place to ensure Personal Information is collected, used, stored and disclosed appropriately, securely, and only with proper authorisation.

3. Policy Scope/Coverage

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

4. Policy Statement

- 4.1. College resources must not be used to access material where content would be inconsistent with the Vision and Values of Canterbury College.
- 4.2. Users must not use services in any way that is contrary to the law or breaches the College's Code of Conduct.
- 4.3. Users shall not access any objectionable or offensive material, illegal content or material inappropriate to an educational or work environment. Users shall not create, engage in or post or forward defamatory, inaccurate, personal, sensitive, abusive, obscene, profane, sexual, threatening, offensive or illegal material on any social media or College platforms.
- 4.4. Email messages or attachments that contain, or are reasonably suspected to contain, offensive material or suspected virus must not be opened or sent.
- 4.5. The Network Administrator may close an account at any time or as requested by Principal or Head of Sub-School.
- 4.6. Users who suspect or know of inappropriate use must report such use to the Head of Sub-School or advise the IT Department.
- 4.7. Any person identified as a security risk may be denied access to Canterbury College technology services at the discretion of the Principal.
- 4.8. A breach of this policy may result in disciplinary action, up to and including dismissal (for employees) or suspension/exclusion (for students). In addition, individuals may be subject to civil or criminal action where their conduct breaches applicable laws.
- 4.9. The College reserves the right to monitor user activity to ensure adherence to the principles of this policy and 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 guidelines.
- 4.10. Users must not publish identifying information or images of students except in accordance with College-approved consent processes and delegated authorisations.
- 4.11. The College upholds the Australian Privacy Principles and Data Protection guidelines and enforces data breach protection measures. The College expects all

users to comply with the privacy, data protection and information security requirements set out in this policy and related College procedures.

- 4.12. All attempts should be made to keep information secure. A common means of gaining illegal access to protected data is through user credentials. Users are required to select passwords that are not easy to guess or to use paraphrases. Users must comply with the College Password Standards.

5. Data Protection and Privacy

Canterbury College collects, uses and stores a range of personal and sensitive information relating to students, employees, parents/guardians, partners and suppliers. This includes any prospective or past students and employees. Protecting this information is essential to maintaining the trust of our community, safeguarding the privacy and safety of individuals — particularly children — and meeting the College's legal obligations under the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles. All Users share responsibility for handling data correctly, using it only for legitimate purposes, and ensuring that Personal Information and Personally Identifiable Information (PII) is not accessed, shared or disclosed without proper authorisation. All users must ensure technology is used in a manner consistent with the College's Child Safety Action Plans and commitment to child safety.

- 5.1. Personal and sensitive information must only be collected, accessed, used or disclosed for legitimate College purposes and in accordance with the Australian Privacy Principles and the *Privacy Act 1988 (Cth)*.
- 5.2. Users must only access Personal Information or PII that is necessary for their role. Accessing, browsing or retrieving information without a legitimate need — even where access is technically possible — is a breach of this policy.
- 5.3. Personal Information must not be shared, forwarded, copied or disclosed to any person, internally or externally, without appropriate authorisation and, where required, the informed consent of the individual concerned or their parent/guardian.
- 5.4. Where consent is required to collect or use an individual's information — including images, video or other identifying material of students — that consent must be obtained and recorded before the information is used, and use must remain within the scope of the consent given.
- 5.5. Personal Information and PII must be stored securely, whether in physical or digital form, and protected by appropriate safeguards such as strong passwords, multi-factor authentication with the exception of students, and restricted access controls. Refer to the College's policy on Passwords.
- 5.6. Multifactor authentication must be enabled on College systems wherever supported and required by the College
- 5.7. Personal Information must not be transferred to, or stored on, personal devices, personal email accounts, unauthorised cloud services or removable media. Only College-approved systems and applications may be used to store or process College data.
- 5.8. Care must be taken when using third-party, online or artificial intelligence (AI) tools. Personal Information, sensitive information or confidential College data must not be entered into any external service that has not been approved by the College, as this may result in unauthorised disclosure.
- 5.9. Particular care must be applied to information relating to children. Identifying information or images of students must not be published, shared or stored other

- than in accordance with this policy and with the written consent of the Principal.
- 5.10. Personal Information must only be retained for as long as it is required for its intended purpose or as required by law and must be disposed of securely when it is no longer needed.
- 5.11. Any actual, suspected or potential data breach, including loss, theft, unauthorised access, or accidental disclosure of Personal Information, must be reported immediately to the IT Department so it can be assessed and managed in accordance with the College's data breach response obligations and, where applicable, the Notifiable Data Breaches (NDB) scheme.

6. Intellectual Property and Data Ownership

- 6.1. All data, records, documents, communications, and information created, collected, stored, or processed in the course of employment remain the Intellectual property of the College. This includes, but is not limited to, emails, student and staff information, reports, databases, learning materials, policies, procedures, and any other College-related digital or physical assets.
- 6.2. Employees and authorised users are entrusted with access to this information solely for legitimate College purposes.
- 6.3. College data must not be removed, copied, transferred, disclosed, or retained outside authorised College systems or premises without prior approval.
- 6.4. Upon cessation of employment or engagement, all College property, including electronic records and emails, must remain with the College and be returned or surrendered as required.

7. Artificial Intelligence (AI)

- 7.1. Canterbury College acknowledges and supports the responsible use of artificial intelligence across the organisation to enhance learning, teaching, and administrative functions.
- 7.2. All users must adhere to the following principles when utilising AI tools:
- 7.2.1. Users are expected to handle data responsibly, ethically, and securely at all times. Care must be taken to prevent the disclosure of personally identifiable information (PII) in any public or unsecured context.
- 7.2.2. All AI-generated content must be thoroughly reviewed, validated, and approved by the originating user before dissemination or publication. Users retain full responsibility for ensuring the accuracy, appropriateness, and compliance of all AI-generated materials with applicable legislation and College policies
- 7.3. Should clarification be required regarding AI usage, responsible data handling, or policy compliance, users are encouraged to contact the IT Department.

8. Guidelines/Procedure/Process

- 8.1. Users of technology need to do so with the intent to meet the College's high

expectations. The College's high standard of expectations extends to the use of its resources outside regular hours, including when utilised offsite and over term breaks.

- 8.2. When users login into the College devices, they agree to this user agreement, signifying their acceptance of and compliance with the terms and conditions governing the use of ICT services at the College.
- 8.3. Users are expected to obey copyright laws and the intellectual property of third parties.
- 8.4. Misuse, damage, or intention to harm College resources or others' files may result in prosecution and school-level consequences, including suspension or expulsion for students and disciplinary measures including dismissal for employees.
- 8.5. Use of College resources for offensive communication, including racist, vulgar, derogatory, or obscene content, can lead to legal action, suspension, or exclusion, covering websites, social media, email, and SMS.
- 8.6. Content linked to Canterbury College, using naming or images, requires College approval. Offensive or inappropriate content may lead to legal action and school-level consequences, including suspension or exclusion.
- 8.7. Unauthorised recording, publication or distribution of images, video or audio involving students, staff or College activities may result in disciplinary action in prosecution and for students, school-level consequences, such as suspension or expulsion.
- 8.8. The College reserves the right to examine its computer network to ensure compliance with this policy.
- 8.9. Personal devices brought to school or school events are brought at the owner's risk. The College assumes no liability for their care or security.
- 8.10. Students in Prep – Year 6 must register their phone at the Junior School Administration.
- 8.11. No phones are to be on the person of any Senior School student from 8:30am until 3:15pm, during the school day.
 - 8.11.1. Students in Years 7-9 must hand in their phone at Senior School Administration before school and collect after school.
 - 8.11.2. Students in Years 10-12 must leave their phones in their locker.
- 8.12. Devices including meta glasses, phones or cameras are not to be used at College sanctioned events or activities or to produce images, unless authorised in writing by the College in support of the educational program.

9. Review

- 9.1. This policy and its associated procedures, quick reference guides and protocols will be reviewed every two years. Canterbury College, however, reserves the right to review this policy at any time.

Version Number:	V1.02026
Policy Library:	College Operations
Responsible Officer	Director of Business and Finance
Approval Authority:	Principal

Last Approval Date:	31 August 2026
Review Date:	31 August 2027
Related Policies/Procedures:	Privacy Policy Data Retention Framework Canterbury College Child Safe Plan Canterbury Early Learning Child Safe Plan Canterbury College Commercial Child Safe Plan Canterbury Student Device Agreement
Acknowledgements:	Privacy Act 1988 (Cth) Australian Privacy Principles (APPs) Notifiable Data Breaches (NDB) scheme