Blackheath & Thornburgh College

PRIVACY POLICY

Review Procedure

The Board and Principal will review the policy as required. The review schedule is directed in response to organisational and/or legislative changes and requirements. The review will be undertaken in consultation with employees and other relevant parties. All relevant persons will be made aware of changes made because of the review.

This policy will be reviewed if:

- There are changes in the workplace that may affect the policy;
- The policy is not effective;
- There are legislative changes that affect the policy; or
- There is a breach of this policy.

This policy is reviewed within 14 months of last approval.

Document Number:	HR01_01a
Topic:	Privacy
Approval Authority:	Board of Directors
Document Owner	Blackheath & Thornburgh College
Last Approval Date:	May 2026
Review Date:	May 2027
Audience:	All employees, students, volunteers, contractors, visitors and stakeholders
Related Policies	Complaint Handling Policy & Procedure Social Media Policy Information Communication & Technology Policy Data Breach Response Plan Generative Artificial Intelligence Policy
Document Web Links:	https://www.oaic.gov.au/privacy/australian-privacy-principles/
Notes:	

Purpose

Blackheath & Thornburgh College is bound by the Australian Privacy Principles ('APPs') contained in the *Privacy Act 1988* (Cth) (the Privacy Act). This Privacy Policy sets out how the College uses and manages personal information provided to or collected by it.

Policy Details

The Privacy Act recognises the importance of protecting the personal information of individuals. It contains a set of rules (the APPs) that govern how organisations collect, store, use and disclose personal information. The College adheres to the thirteen guidelines as stated in the privacy principles, outlined in Appendix 1. The Privacy Act also allows an individual to make a complaint about any organisations breach of the privacy principles.

The College may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the College operations and practices and to make sure it remains appropriate to the changing College environment.

Exemption in relation to employee records
Under the Privacy Act, the APPs do not apply to an employee record held by the employing entity. As a result, this Privacy Policy does not apply to the College's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the College and employee.

In some circumstances, the College's handling of records in relation to current and former employment relationships is exempt from the APPs (for further details please refer to s7B(3) of the Privacy Act).

What kinds of personal information does the College collect and how does the College collect it?
The type of information the College collects and holds includes (but is not limited to) personal information, including health and other sensitive information, about:

- students and parents and/or guardians ('parents') before, during and after the course of a student's enrolment at the College:
    - name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;
    - parents' education, occupation and language background;
    - medical information (e.g. details of disability and/or allergies, absence notes, medical reports and names of doctors);
    - conduct and complaint records, or other behaviour notes, and school reports; information about referrals to government welfare agencies;
    - counselling reports;
    - health fund details and Medicare number;
    - any court orders;
    - volunteering information; and
    - photos and videos at school events.
- job applicants, staff members, volunteers and contractors:
    - name, contact details (including next of kin), date of birth, and religion;
    - information on job application;
    - professional development history;
    - salary and payment information, including superannuation details;
    - medical information (e.g. details of disability and/or allergies, and medical certificates);
    - complaint records and investigation reports;
    - leave details;
    - photos and videos at school events;
    - workplace surveillance information; and
    - work emails and private emails (when using work email address) and internet browsing history.
- other people who come into contact with the College including name and contact details and any other information necessary for the particular contact with the College.

Personal information you provide
The College will generally collect personal information held about an individual by way of forms filled out by parents or students, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than parents and students provide personal information.

Personal information provided by other people
In some circumstances the College may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another school.

Personal information from other sources
The College may collect personal information through surveillance activities (such as CCTV security cameras) and student email monitoring.

How will the College use the personal information you provide?
The College will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected by you, or to which you have consented.

Students and Parents
In relation to personal information of students and parents, the College's primary purpose of collection is to enable the College to provide schooling to students enrolled at the school, exercise its duty of care, and perform necessary associated administrative activities, which will enable students to take part in all the activities of the College. This includes satisfying the needs of parents, the needs of the students and the needs of the College throughout the whole period the student is enrolled at the College.

The purposes for which the College uses personal information of students and parents include:

- to keep parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration of the College;
- looking after student's educational, social and medical wellbeing;
- seeking donations and marketing for the College; and
- to satisfy the College's legal obligations and allow the school to discharge its duty of care.

In some cases where the College requests personal information about a student or parent, if the information requested is not provided, the College may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

On occasions information such as academic and sporting achievements, student activities and similar news is published in College newsletters and magazines, on our intranet and on our website, this may include photographs and videos of student activities such as sporting events, school camps and school excursions. The College will obtain ongoing permission (once given, this consent will be amended or revoked only upon receipt of written notification from the parent/guardian who originally gave it or individual if over 18 years of age) from the student's parent or guardian (and from the student if appropriate) if we would like to include such photographs or

videos or other identifying material in our promotional material or otherwise make this material available to the public such as on the internet.

Job applicants, staff members and contractors
In relation to personal information of job applicants, staff members and contractors, the College's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor.

The purposes for which the College uses personal information of job applicants, staff members and contractors include:

- in administering the individual's employment or contract;
- for insurance purposes;
- seeking donations and marketing for the College; and
- to satisfy the College's legal obligations, for example, in relation to child protection legislation.

Volunteers
The College also obtains personal information about volunteers who assist the College in its functions or conduct associated activities, such as alumni associations, to enable the College and the volunteers to work together.

Marketing and Fundraising
The College treats marketing and seeking donations for the future growth and development of the College as an important part of ensuring that the College continues to provide a quality learning environment in which both students and staff thrive. Personal information held by the College may be disclosed to organisations that assist in the College's fundraising, for example, the Blackheath & Thornburgh Foundation or alumni organisation, or, on occasions, external fundraising organisations.

Parents, staff, contractors and other members of the wider College community may from time to time receive fundraising information. College publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

If you would like to opt-out of direct marketing, please contact the Marketing & Events Manager on (07) 4787 5100 or via email at marketing@btc.qld.edu.au

Who might the College disclose personal information to and store your information with?
The College may disclose personal information, including sensitive information, held about an individual for educational, legal, administrative, marketing and support purposes. This may include disclosing this information to:

- another school or staff at another school;
- government departments (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the College, including specialist visiting teachers, sports coaches, volunteers, counsellors and providers of learning and assessment tools;

- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- people providing administrative and financial services to the College;
- recipients of College publications, such as newsletters and magazines;
- students' parents or guardians;
- anyone you authorise the College to disclose information to; and
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

Sending and storing information overseas
The College may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, the College will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); and
- otherwise complying with the APPs or other applicable privacy legislation.

The College may use online or 'cloud' service providers to store personal information and to provide services to the College that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's server which may be situated outside Australia.**

An example of such a cloud service provider is Google. Google provides the 'Google Apps for Education' (GAFE) including Gmail, and stores and processes limited personal information for this purpose. College personnel and the AIS and its service providers may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering GAFE and ensuring its proper use.

**The data centres where the personal information is likely to be kept are located in the USA, Taiwan, Singapore, Ireland, Netherlands and Belgium.

Sensitive information
In referring to 'sensitive information', the College means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.
Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is required by law.

Management and security of personal information
The College's staff are required to respect the confidentiality of students' and parents' personal information and the privacy of individuals. The College has in place steps to protect the personal information the College holds from misuse, interference and loss, unauthorised access, modification

or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

Data breaches

In the event that the College becomes aware of, or has reasonable grounds to suspect, an unauthorised access to, or disclosure of, personal information held by the College, or the loss of personal information where the loss is likely to result in unauthorised access or disclosure of personal information, the College will take appropriate, prompt action to investigate the breach and take remedial action in accordance with the College's Data Breach Response Plan to:

- confirm, contain and keep records of the data breach and do a preliminary assessment;
- assess the data breach and evaluate the risks associated with the breach including if there has been an 'eligible data breach';
- consider notification requirements (the Office of Australian Information Commissioner ('OAIC') and any affected individuals), also outlined below; and
- review the data breach or eligible data breach to prevent future breaches.

It will be deemed that an 'eligible data breach' has occurred if:

- there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals (the affected individuals);
- a reasonable person would conclude there is a likelihood of serious harm to any affected individuals as a result; or
- the information is lost in circumstances where:
    - unauthorised access to, or unauthorised disclosure of, the information is likely to occur; or
    - assuming unauthorised access to, or unauthorised disclosure of, the information was to occur, a reasonable person would conclude that it would be likely to result in serious harm to the affected individuals.

Serious harm may include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

What must the College do in the event of an 'eligible data breach'?

If the College suspects that an eligible data breach has occurred, it will carry out a reasonable and expedient assessment/investigation within 30 days.

If such an assessment/investigation indicates there are reasonable grounds to believe an eligible data breach has occurred, then the College will be required to lodge a statement to the Privacy Commissioner. Where practical to do so, the College will also notify the affected individuals. If it is not practicable to notify the affected individuals, the College will publish a copy of the statement on its website or publicise it in another manner.

Exception to notification obligation

An exception to the requirement to notify will exist if there is a data breach and immediate remedial action is taken, and as a result of that action:

- there is no unauthorised access to, or unauthorised disclosure of, the information; and

- there is no serious harm to affected individuals, and as a result of the remedial action, a reasonable person would conclude the breach is not likely to result in serious harm.

Access and correction of personal information
Under the Privacy Act, an individual has the right to seek and obtain access to any personal information which the College holds about them and to advise the College of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Students will generally be able to access and update their personal information through their parents, but older students may seek access and correction themselves.

To make a request to access or to update any personal information the College holds about you or your child, please contact the College in writing via email at reception@btc.qld.edu.au . The College may require you to verify your identity and specify what information you require. The College may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the College will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

The College will take reasonable steps to ensure that any personal information is accurate, up to date, complete, relevant and not misleading.

Consent and rights of access to the personal information of students
The College respects every parent's right to make decisions concerning their child's education. Generally, the College will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The College will treat consent given by parents as consent given on behalf of the student and notice to parents will act as notice given to the student. As mentioned above, parents may seek access to personal information held by the College about them or their child by contacting the College. However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the the College's duty of care to a student.

The College may, at its discretion, at the request of a student, grant that student access to information held by the College about them, or allow a student to give or withhold consent to the use of their personal information, independently of their parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances warrant it.

Enquiries and complaints
If you would like further information about the way the College manages the personal information it holds or wish to make a complaint in circumstances where the College may have breached of the APPs, please contact the Principal or follow the process outlined in the College's Complaint Handling Policy & Procedure. The College will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

APPENDIX 1

Australian Privacy Principles (APPs)

APP 1: Open **and transparent management of personal information**
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2: **Anonymity and pseudonymity**
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3: **Collection of solicited personal information**
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information.

APP 4: Dealing with unsolicited personal information
Outlines how APP entities must deal with unsolicited personal information.

APP 5: Notification of the collection of personal information
Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.

APP 6: Use or disclosure of personal information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7: Direct marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8: Cross-border disclosure of personal information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9: Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10: Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11: Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12: Access to personal information
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13: Correction of personal information
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.