

Privacy Policy

Contents

Privacy Policy	3
Legislation	3
Related Alta-1 Policies	3
Commitment.....	3
Scope.....	3
Responsibilities	4
Definitions.....	4
What kind of information does Alta-1 College collect and how does the school collect it? ..	5
Purposes for which the College collects, uses, and discloses information.....	6
Data Breaches – Notifiable Data Breaches Scheme	9
Access and Correction of Personal Information.....	10
Consent and Rights of Access to the Personal Information of Students	10
Implementation.....	11
Contact, Enquiries and Complaints.....	11
Related Procedures.....	11

Privacy Policy

Legislation

[School Education Act 1999](#)

[School Education Regulations 2000 \(WA\)](#)

[Australian Education Act 2013 \(Cth\)](#)

[Australian Privacy Principles](#)

[Privacy Act 1988 \(Cth\)](#)

Related Alta-1 Policies

This policy should be read in conjunction with the Alta-1 College:

Child Protection Policy

Staff Complaints & Grievance Policy

Responsible use of ICT Policy

Staff Code of Conduct

Commitment

Alta-1 College Ltd is committed to managing personal, sensitive and health information in accordance with the Australian Privacy Principles under the *Privacy Act 1988* (Cth) and in accordance with any other applicable privacy laws.

This document sets out our policies for managing your personal, sensitive and health information and is referred to as our **Privacy Policy**.

Alta-1 College may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to Alta-1's operations and practices, and to make sure it remains appropriate to the changing school environment.

Scope

This policy applies to the entire school community when collecting, holding, accessing and using personal and sensitive information from and about, but not limited to:

- Current and prospective students
- Current and prospective parents/guardians
- Current and prospective staff
- Current and prospective Board members
- Past students and staff
- Current and prospective donors
- Current and prospective suppliers and contractors
- Volunteers
- Users of the School's facilities and services
- Attendees at events or activities.

Exception in relation to employee records

Under the *Privacy Act 1988* (Cth), the Australian Privacy Principles do not apply to employee records. 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.

Responsibilities

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.

The following are responsibilities required of staff and/or other personnel of the College to ensure protection of personal information:

Employees are required to:

- be aware of the requirements for protection of personal information as outlined in this Privacy Policy aligns with the *Privacy Act 1988* (Cth)
- report suspected privacy breaches to their line manager
- action request for information applications in accordance with this procedure

Line Manager's are required to:

- escalate any reported privacy breaches as necessary. (See Contact, Enquiries and Complaints)

The Director of Corporate Services is required to:

- ensure their employees are aware and adhere to the requirements for protection of personal information as outlined in the Alta-1 College Privacy Policy which aligns with the *Privacy Act 1988* (Cth)
- refer reported privacy breaches to the relevant Government authority

Definitions

APPs means Australian Privacy Principles under the *Privacy Act 1988* (Cth).

The Act means the *Privacy Act 1988* (Cth).

The College means Alta-1 College Ltd

Employee record in relation to an employee, means a record of personal information relating to the employment of the employee. This includes health information and Personal Information about any of the following:

- engagement, training, disciplining or resignation of the employee
- termination of the employment of the employee
- terms and conditions of the employee
- employee's personal and emergency contact details
- employee's performance or conduct
- employee's hours of employment
- employee's salary or wages
- employee's membership of a professional or trade association
- employee's trade union membership
- employee's recreation, long service, sick, personal, maternity, paternity or other leave
- employee's taxation, banking or superannuation affairs

Individual, in relation to Personal Information, means the individual to whom the information relates.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Examples of Personal Information can include (without limitation) the name, age and date of birth of the individual.

Primary Purpose means the purpose for which the Personal Information was collected.

Privacy Officer is the person appointed to the position of Privacy Officers in the College, whose contact details are available in section 11 of this Privacy Policy.

Secondary Purpose means the use of Personal Information for a purpose that is not the Primary Purpose.

Sensitive Information means:

- A. Information or an opinion about an individual's:
 - i. racial or ethnic origin, or
 - ii. political opinions, or
 - iii. membership of a political association, or
 - iv. religious beliefs or affiliations, or
 - v. philosophical beliefs, or
 - vi. membership of a professional or trade association, or
 - vii. membership of a trade union, or
 - viii. sexual orientation or practices, or
 - ix. criminal record,
 that is also personal information; or
- B. Health information about an individual; or
- C. Genetic information about an individual that is not otherwise health information; or
- D. Biometric information that is to be used for the purposes of automated biometric verification or biometric identification; or
- E. Biometric templates.

What kind of information does Alta-1 College collect and how does the school collect it?

The type of information the College collects and holds includes (but is not limited to) personal information, including medical and other sensitive information, about:

- students and parents and/or carers, before, during and after the course of a student's enrolment at the College,
- job applicants, staff members, volunteers and contractors, and
- other people who come into contact with the College via the College website or social media, on campus, or over the phone.

For example:

In relation to students:

- 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, vaccinations, 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;
- court orders;
- photos and videos at school events;
- biometric data;
- student emails and private emails when using student email address and internet browsing history.

In relation to job applicants, staff members, volunteers, 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;
- work emails and private emails (when using work email address) and Internet browsing history

How does the College collect personal information?

The College will generally collect personal information about an individual through the completion of forms (including digital) by current and prospective staff, parents/carers or students, face-to-face meetings and interviews, emails and/or telephone calls.

On occasion, people other than parents/carers and students may provide personal information.

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.

Purposes for which the College collects, uses, and discloses information

The College will use personal information it collects from you for the primary purposes set out below and for any secondary purposes that are related to the primary purpose and reasonably expected by you, or to which you have consented.

Students and Parents/Carers

In relation to personal information of students and parents/carers, the College's primary purpose of collection is to enable the College to provide education for the student, exercise its duty of

care, and perform necessary associated administrative activities, which will enable the student to take part in all the activities of the College. This includes satisfying the needs of parents/carers, student needs, 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/carers include:

- to keep parents/carers informed about matters related to their child's schooling, through correspondence, newsletters and other College publications
- providing schooling and schooling activities
- making required reports to government authorities
- day-to-day administration of the College
- looking after the student's health, educational, social and wellbeing of the student
- seeking donations and marketing for the College
- to satisfy the College's legal obligations and allow the College to discharge its duty of care

In some cases where the College requests personal information about a student or parent/carer, 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 School newsletters and magazines, on our intranet, and on our website and social media platforms. This may include photographs and videos of student activities such as sporting events, school camps and excursions.

The College will obtain permissions from the student's parent or guardian (and from the student if appropriate) if we would like to include such photographs, videos, or other identifying material in our promotional material or if we would like to make it 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 the person is successful, to engage the applicant, staff member or contractor as the case may be.

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

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

Volunteers

The College also collects personal information about volunteers who assist the College in its functions or conduct associated activities, to enable the College and the volunteers to work together in a safe and supportive environment.

Marketing

The College considers marketing an important part of its future growth and development and 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, including external fundraising organisations.

Parents/Carers, 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.

Disclosure of Personal Information

The College may disclose personal information, including sensitive information, held about any individual for educational, legal, administrative, marketing and support purposes.

For example, this may include disclosing 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, 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 Alta-1 College to disclose information to
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws

Sending and Storing Information Overseas

Alta-1 College may disclose personal information about an individual to overseas recipients, for example, to facilitate a college trip or student exchange. However, the College will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual, and in some cases, this will be implied, or
- otherwise complying with the Australian Privacy principles 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.

The data centres where the personal information is likely to be kept are located in Australia and Singapore.

Management and Security of Personal information

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.

College 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 held it from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods.

The various methods used by the College include:

Hard Copy Files:

- Hard copy files are to be stored in locked storage, be it onsite or offsite. Access to these records is restricted to authorised College employees.
- All authorised College employees must ensure that all papers and files relating to College employees are stored in locked areas at night, when authorised employees are absent from the office or at other times when authorised employees are not working on such papers or files.
- Any destruction of copies of documents or unwanted pieces should be by way of secure destruction bin or shredding.

Digital Files:

- In relation to the ICT Security protocols identified in the Essential 8 Framework, the College commits to operate at 1.5 in each of the categories.

Data Breaches - Notifiable Data Breaches Scheme

Unauthorised access occurs where personal information is accessed by someone who is not permitted to have access to that information. For example, by an employee of the College, an independent contractor, or a third party by 'hacking'.

Unauthorised disclosure occurs when the College, intentionally or unintentionally, makes personal information accessible or visible to others outside of the College and releases the information in a way that is not permitted by the Privacy Act. This includes unauthorised disclosures by staff members.

A Data Breach is an Eligible Data Breach (EDB) if it is likely to result in serious harm to an individual/s whose information is involved in the Data Breach. The following three criteria need to be satisfied to be an 'eligible data breach':

- there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals, and
- a reasonable person would conclude there is a likelihood of serious harm to any affected individuals as a result, and
- the information is lost in circumstances where:
 - unauthorised access to, or unauthorised disclosure of, the information is likely to occur,

- assuming unauthorised access to, or unauthorised closure 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 the College must do in the event of an eligible data breach

The College must immediately act to contain a suspected or known 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 the 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 (**Commissioner**). Where practical to do so, the school entity will also notify the affected individuals.

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
- 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

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

Under the *Privacy Act 1988* (Cth), an individual has the right to obtain access to any personal information which the College holds about them. They may also advise the College of any perceived inaccuracy. Students will generally be able to access and update their personal information through their parents/carers but can seek access and correction themselves.

There are some exceptions to this right set out in the Act.

Permission to gain access or update any personal information the College holds about an individual, must be made to Director of Corporate Services in writing. If an individual makes a request, the College may require them to verify their identity and set out specifically what information is required. The College may charge a fee to cover the cost of verifying an 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 the College cannot provide access to the requested information or considers that it is unable to do so because of a relevant exception, it will provide written notice explaining the reasons for refusal.

Consent and Rights of Access to the Personal Information of Students

The College respects every parent/carer'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/carers. The College will treat consent

given by parents/carers as consent given on behalf of the student and notice to parents will act as notice given to the student.

Parents/carers may seek access to personal information held by the College about them or their child by contacting the Regional Principal. 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 College's duty of care to the student.

The College may, at its discretion, grant a student access to their information or allow a student to give or withhold consent to the use of their personal information, independent of their parents/carers. The student must make the request themselves and permission would normally be given when the maturity of the student and/or the students' personal circumstances warrant this.

Implementation

- Staff will follow the necessary procedures to ensure compliance with the policy.
- The policy will be made available through the College's internal staff SharePoint site.
- All staff are to be made aware of this policy and any relevant documentation, forms, and workflows.

Contact, Enquiries and Complaints

Further information about the way Alta-1 College manages the personal information it holds can be obtained by contacting the Risk and Compliance Coordinator via email to:

riskandcompliance@alta-1.wa.edu.au

Any complaint about a possible breach of the Australian Privacy Principles should be directed to the Risk and Compliance Coordinator via email to:

riskandcompliance@alta-1.wa.edu.au

The College will investigate any complaint and will notify the complainant of the outcome of the complaint as soon as is practicable after it has been made.

Related Procedures

- Suspected Data Breach Procedure

Policy Details and Document Management

Privacy Policy

Author: Director of Corporate Services

Approved by: Alta-1 College Board

Published: 21/02/2025

Review Date: February 2025

Policy Level		Dissemination	For Application	For Information
College Board	<input checked="" type="checkbox"/>	College Board	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Chief Executive Officer	<input type="checkbox"/>	Chief Executive Officer	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Executive Team	<input type="checkbox"/>	Executive Leadership	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Senior Leadership Team	<input type="checkbox"/>	Senior Leadership	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		Central Administration	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		Regional Administration	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		Teaching Staff	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		Campus Staff	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		Therapeutic Staff	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		Community (Parents/Students)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Access				
Open	<input checked="" type="checkbox"/>			
Restricted	<input type="checkbox"/>			

Version Control & Genealogy

Version	Published	Author Changes	Summary of Changes including replacement and/or cancellation or suspension of policy.
1	December 2020	M Bishop	Document created. Privacy Policy.
2	February 2025	L Healy & Adam Butler	Document rewritten to bring into alignment with current legislation. New format adopted.