Privacy Policy

In the course of Aitken College's activities, we manage and protect personal information in accordance with the Privacy and Data Protection Act 2014 (Cth) (Privacy Act) and the 13 Australian Privacy Principles (APPs) as well as the requirements of the Health Records Act (Vic) (the Health Privacy Principles).

What is personal information and how do we collect it?

Personal information is information or an opinion about an individual from which they can be reasonably identified. Depending on the circumstances, we may collect personal information from an individual in their capacity as a student, contractor, volunteer, stakeholder, job applicant, alumni, visitors or others that come into contact with the school.

In the course of providing services we may collect and hold:

• **Personal Information** including names, addresses and other contact details; dates of birth; next of kin details; photographic images; attendance records and financial information.
• **Sensitive Information** (particularly in relation to student and parent records) including government identifiers (such as TFN), religious beliefs, nationality, country of birth, professional memberships, family court orders and criminal records.
• **Health Information** (particularly in relation to student and parent records) including medical records, disabilities, immunisation details and psychological reports.

As part of our recruitment processes for employees, contractors and volunteers, we may collect and hold:

• **Personal Information** including names, addresses and other contact details, dates of birth, financial information, citizenship, employment references, regulatory accreditation, media, directorships, property ownership and driver's licence information.
• **Sensitive Information** including government identifiers (such as TFN), nationality, country of birth, professional memberships, family court orders and criminal records.
• **Health Information** (particularly in relation to prospective staff and student records) including medical records, disabilities, immunisation details and psychological reports.

Generally, we will seek consent from the individual in writing before we collect their sensitive information.

It is noted that employee records are not covered by the APPs or the Health Privacy Principles where they relate to current or former employment relations between the school and the employee. However, a current or former employee's health records are covered by the Victorian Health Privacy Principles.

Collection of Personal Information

The collection of personal information depends on the circumstances in which Aitken College is collecting it. If it is reasonable and practical to do so, we collect personal information directly from the individual.

Solicited Information

Aitken College has, where possible, attempted to standardise the collection of personal information by using specifically designed forms (e.g. an Enrolment Form or Health Information Disclosure Form). However, given the nature of our operations we also receive personal information by email, letters, notes, via our website, over the

telephone, in face-to-face meetings, through financial transactions and through surveillance activities such as the use of CCTV security cameras or email monitoring.

We may also collect personal information from other people (e.g. a third-party administrator, referees for prospective employees) or independent sources. However, we will only do so where it is not reasonable and practical to collect the personal information from the individual directly.

Unsolicited Information

Aitken College may be provided with personal information without having sought it through our normal means of collection. This is known as "unsolicited information" and is often collected by:

• Misdirected postal mail – Letters, Notes, Documents
• Misdirected electronic mail – Emails, electronic messages
• Employment applications sent to us that are not in response to an advertised vacancy
• Additional information provided to us which was not requested.

Unsolicited information obtained by Aitken College will only be held, used and or disclosed if it is considered as personal information that could have been collected by normal means. If that unsolicited information could not have been collected by normal means then we will destroy, permanently delete or de-identify the personal information as appropriate.

Collection and use of sensitive information

We only collect sensitive information if it is

- reasonably necessary and we have the individual's consent,
- necessary to lessen or prevent a serious threat to life, health or safety,
- another permitted situation, or
- another permitted health situation.

We may share sensitive information to other entities in our organisation structure for primary purposes. Our primary purpose is for the College to provide our products or services which includes an education and support.

How do we use personal information?

Aitken College only uses personal information that is reasonably necessary for one or more of our functions or activities (the primary purpose) or for a related secondary purpose that would be reasonable expected by you, or for an activity or purpose to which you have consented.

Our primary uses of personal information include, but are not limited to:

• providing education, pastoral care, extra-curricular and health services
• satisfying our legal obligations including our duty of care and child protection obligations
• keeping parents informed as to school community matters through correspondence, newsletters and magazines
• marketing, promotional and fundraising activities
• supporting the activities of school associations such as [Alumni Association]
• supporting the activities of the [School/College foundation]
• supporting community based causes and activities, charities and other causes in connection with the School's functions or activities
• helping us to improve our day-to-day operations including training our staff

• systems development; developing new programs and services; undertaking planning, research and statistical analysis
• school administration including for insurance purposes
• the employment of staff
• the engagement of volunteers.

We will only use or disclose sensitive or health information for a secondary purpose if you would reasonably expect us to use or disclose the information and if the secondary purpose is directly related to the primary purpose.

We may share personal information to related bodies corporate, but only if necessary for us to provide our services.

The College may disclose information about an individual to overseas recipients only when it is necessary, for example to facilitate a student exchange program. The College will not however send information about an individual outside of Australia without their consent

Aitken College does not use automated computer programs, such as AI, to make decisions or take actions that could significantly impact an individual's rights and does not insert personal information into such programs.

Storage and Security of Personal Information, including with Cloud Service Providers

Aitken College stores Personal Information in a variety of formats including databases, hard copy files, personal devices, including laptop computers, third party storage providers such as cloud storage facilities and paper based files.

Aitken College takes all reasonable steps to protect the personal information we hold from misuse, loss, unauthorised access, modification or disclosure. These steps include, but are not limited to:

• Restricting access and user privilege of information by staff depending on their role and responsibilities.
• Ensuring staff do not share personal passwords.
• Ensuring hard copy files are stored in lockable filing cabinets in lockable rooms. Staff access is subject to user privilege.
• Ensuring access to Aitken College's premises are secured at all times.
• Implementing physical security measures around the school buildings and grounds to prevent break-ins.
• Ensuring our IT and cyber security systems, policies and procedures are implemented and up to date.
• Ensuring staff comply with internal policies and procedures when handling the information.

• Undertaking due diligence with respect to third party service providers who may have access to personal information, including customer identification providers and cloud service providers, to ensure as far as practicable that they are compliant with the APPs or a similar privacy regime.
• With respect to each cloud service provider, the College has identified where the data is stored, the type of personal information that is stored, whether the data is secured, whether the provider is subject to the same or similar privacy laws and what risk mitigation strategies are in place.
• The destruction, deletion or de-identification of personal information we hold that is no longer needed, or required to be retained by any other laws.

Our public website may contain links to other third-party websites outside of Aitken College. Aitken College is not responsible for the information stored, accessed, used or disclosed on such websites and we cannot comment on their privacy policies.

The College undertakes an annual personal information audit where an assessment is made on:

- whether the personal information the College requests, or holds, is necessary
- whether personal information is stored securely, both physically and electronically, including through the College's chosen cloud service providers
- what risk strategies are in place at the College and with the chosen cloud service providers

The College maintains up-to-date with patching of servers and continues to have a double stacked firewall. Total backup solutions are run daily with snapshots conducted every 15 minutes.

Responding to data breaches

Aitken College will take appropriate, prompt action if we have reasonable grounds to believe that a data breach may have, or is suspected to have occurred. Depending on the type of data breach, this may include a review of our internal security procedures, taking remedial internal action, notifying affected individuals and the Office of the Australian Information Commissioner (OAIC).

If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

Disclosure of personal information

Personal information is used for the purposes for which it was given to Aitken College, or for purposes which are directly related to one or more of our functions or activities. Personal information may be disclosed to government agencies, other parents, other schools, recipients of school publications, visiting teachers, counsellors and coaches, our services providers, agents, contractors, business partners, related entities and other recipients from time to time, if the individual:

• Has given consent; or
• Would reasonably expect the personal information to be disclosed in that manner.

Aitken College may disclose personal information without consent or in a manner which an individual would reasonably expect if:

• We are required to do so by law.
• The disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety.
• Another permitted general situation applies.
• Disclosure is reasonably necessary for a law enforcement related activity.
• Another permitted health situation exists.

Disclosure of your personal information to overseas recipients

Personal information about an individual may be disclosed to an overseas organisation in the course of providing our services, for example when storing information with a "cloud service provider" which stores data outside of Australia or to facilitate a school exchange. We will however take all reasonable steps not to disclose an individual's personal information to overseas recipients unless:

• we have the individual's consent (which may be implied);
• we have satisfied ourselves that the overseas recipient is compliant with the APPs, or a similar privacy regime;
• we form the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or
• we are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

Personal information of students

The Privacy Act does not differentiate between adults and children and does not specify an age after which individuals can make their own decisions with respect to their personal information.

At Aitken College we take a common-sense approach to dealing with a student's personal information and generally will refer any requests for personal information to a student's parents/carers. We will treat notices provided to parents/carers as notices provided to students and we will treat consents provided by parents/carers as consents provided by a student.

We are however cognisant of the fact that children do have rights under the Privacy Act, and that in certain circumstances (especially when dealing with older students and especially when dealing with sensitive information), it will be appropriate to seek and obtain consents directly from students. We also acknowledge that there may be occasions where a student may give or withhold consent with respect to the use of their personal information independently from their parents/carers.

There may also be occasions where parents/carers are denied access to information with respect to their children, because to provide such information would have an unreasonable impact on the privacy of others, or result in a breach of the school's duty of care to the student.

The quality of personal information

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up-to-date, including at the time of using or disclosing the information.

If Aitken College becomes aware that the Personal Information is incorrect or out of date, we will take reasonable steps to rectify the incorrect or out of date information.

Access and correction of personal information

You may submit a request to us to access the personal information we hold, or request that we change the personal information. Upon receiving such a request, we will take steps to verify your identity before granting access or correcting the information.

If we reject the request, you will be notified accordingly. Where appropriate, we will provide the reason/s for our decision. If the rejection relates to a request to change personal information, an individual may make a statement about the requested change and we will attach this to their record.

Complaints

You can make a complaint about how Aitken College manages personal information, including a breach of the APPs or the Health Privacy Principles, by notifying us in writing as soon as possible. We will respond to the complaint within a reasonable time (usually no longer than 30 days) and we make seek further information in order to provide a full and complete response.

If you are not satisfied with our response, you may refer the complaint to the OAIC. A complaint can be made using the OAIC online Privacy Complaint form or by mail, fax or email. A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted.

How to contact us

Aitken College can be contacted about its Privacy Policy or about personal information generally, by:

- Emailing admin@aitkencollege.edu.au
- Calling (03) 9333-9100
- Writing to our Privacy Officer at 1010 Mickleham Road, Greenvale VIC 3059

If practical, you can contact us anonymously (i.e. without identifying yourself) or by using a pseudonym. However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive if it is not practical to do so.

This Privacy Policy is subject to change at any time. Please check our Privacy Policy on our website (www.aitkencollege.edu.au) regularly for any changes.

If you wish to discuss this policy or provide feedback please email admin@aitkencollege.edu.au.

Revision History

Version	Date	Reviewed/Updated by (name)	Position/Title	Approved by
1 (CompliSpace Version)	07/03/2018	Kim Forward	Deputy Principal	Deputy Principal
2	11/4/2019	Josie Crisara	Principal	Principal
2.1	19/03/2020	Josie Crisara	Principal	Principal
2.2	10/03/2021	Kim Forward	Deputy Principal	Deputy Principal
2.3	09/03/2022	Josie Crisara	Principal	Principal
3	17/11/2022	Kim Forward Amy Schembri	Deputy Principal Compliance Manager	Deputy Principal
4	01/03/2023	Kim Forward Amy Schembri College Board	Deputy Principal Compliance Manager	Deputy Principal
4.1	08/03/2024	Josie Crisara	Principal	College Board
5	06/03/2025	Josie Crisara	Principal	College Board
6	15/05/2025	Kim Forward	Deputy Principal	