Privacy Policy

Purpose

This policy outlines how Scotch College (the School) uses and manages personal information.

This policy is also a guide to School staff as to the standards to be applied in respect of handling personal information. It is intended to ensure consistency in the School's approach to privacy.

The School is bound by the Australian Privacy Principles contained in the *Privacy Act 1988* (Commonwealth). The School will collect, use and retain personal information in accordance with those Principles.

The School may, from time to time, review and update this policy to take into account new laws, new technology, and changes to the School's operations and practices.

This document seeks to explain

The legal framework
Those to whom this Policy applies
Definitions: what information we are dealing with?
Principles of how we manage this information:

1. What information is collected and why
2. How we should use it
3. How we should store it
4. How we provide access for those to whom the information belongs
5. How we should dispose of it

What if we have a data breach? (see separate document for flow chart)
A simple guide: What Does This Mean For Me?

Australian Privacy Principles

From 12 March 2014, thirteen Australian Privacy Principles (APPs) replaced the National Privacy Principles and Information Privacy Principles.

The School is required to comply with the APPs.

The APPs set minimum standards that relate to the collection, security, storage, use, correction and disclosure of personal information, as well as access to that information.

The principles are as follows:

- APP 1: Open and transparent management of personal information
- APP 2: Anonymity and pseudonymity
- APP 3: Collection of solicited personal information
- APP 4: Dealing with unsolicited information
- APP 5: Notification of the collection of personal information
- APP 6: Use or disclosure of personal information
- APP 7: Direct marketing
- APP 8: Cross-border disclosure of personal information
- APP 9: Adoption, use or disclosure of 'government related identifiers'
- APP 10: Quality of personal information
- APP 11: Security of personal information
- APP 12: Access to personal information
- APP 13: Correction of personal information

Scope

This policy applies to all current and past students, parents and guardians of students, employees, Council and Sub-Committee Members, consultants, volunteers and contractors of the School.

This policy also applies in relation to all events and activities conducted by the School and events attended by representatives of the School, whether on or off site.

This policy also covers other members of the community who deal with the School.

Definitions

The APPs regulate how the School deals with the following types of information:

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information, regardless of its source. Personal information does not include information about an individual that has been de-identified so that the individual is no longer identifiable.

Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. Sensitive information includes any personal information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. Sensitive information also includes health information.

Health information is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services, and health services provided to an individual currently or in the future. Health information also includes personal information collected in the course of providing a health service.

Principles

1. Collection

Types of personal information collected and held by the School

The type of information the School collects and holds includes (but is not limited to) personal information, including health information 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 School;
- job applicants, staff members, school board members, volunteers and contractors; and
- other people who come into contact with the School.

Some examples of information that the School collects and holds include contact details, student enrolment information, health information and employment history for staff.

Personal information provided by an individual: The School will generally collect personal information held about an individual directly from that individual (or, in the case of a student or prospective student, directly from the student's parents) by way of forms (paper and/or electronic) filled out by parents or students, face-to-face meetings and interviews, on-line surveys, emails and telephone calls.

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

Exception in relation to employee records: Under the Privacy Act the APPs do not apply to an employee record. Accordingly, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the School and an employee.

2. Use of personal information by the School

From time to time, the School will collect, use and disclose personal information for a particular purpose (the primary purpose).

The School may use or disclose the personal information it holds about you for other purposes (secondary purposes) if you (or, in the case of a student, the student's parents) consents to use or disclosure for the secondary purpose.

The School may also use or disclose the personal information it holds about you for a secondary purpose, without specific consent, if the secondary purpose:

- is something you would reasonably expect; and
- is related to the primary purpose (or, in the special case of sensitive information, directly related to the primary purpose).

The following examples may assist.

Students and families

In relation to personal information of students and parents, including prospective students and parents, the School's primary purpose of collection is to enable the School to provide schooling for the student while the student is enrolled at the School.

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

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

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

Job applicants, staff members, Council & Sub-Committee Members and contractors

In relation to personal information of job applicants, staff members, Council & Sub-Committee members and contractors, the School's primary purpose of collection is to assess applications for positions and (if successful) to engage the applicant.

The purposes for which the School uses personal information of job applicants, staff members, Council & Sub-Committee Members and contractors include:

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking donations and marketing for the School; and
- satisfying the School's legal obligations.

Volunteers

The School obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as the Parents & Friends Association, and the Old Collegians Association.

The purposes for which the School uses this personal information include:

- administering and coordinating the activities of these volunteers,
- for insurance purposes;
- seeking donations and marketing for the School; and
- satisfying the School's legal obligations.

Marketing and philanthropy

The information is being collected by Scotch College Adelaide to engage with alumni, donors, partners and friends of the College, and to promote College activities, including events, programs, newsletters and fundraising initiatives, including those for the Scotch College Foundation, Parents & Friends Associations and the Scotch College Old Collegians Association. The information may also be used for analysis, quality assurance and planning purposes and to ensure your interests are met.

The information collected may be disclosed to College's contracted service providers which the College uses to perform services on its behalf. School publications, like newsletters and magazines, may include personal information and may be used for promotional purposes. We will not disclose your personal information to anybody else, unless you have given consent, or we are authorised or required to do so by law. Providing the requested information is not required by law, however, if you choose not to provide it, we may be unable to engage with you or provide you the services requested.

If you wish to inquire about the handling of your personal information, or make a complaint about how we have handled your information, please contact the College.

Disclosure of personal information

For administrative and educational purposes, the School may from time to time disclose personal information and sensitive information held about an individual to:

- another school;
- government departments;
- medical practitioners;
- people providing services to the School, including, but not limited to, specialist visiting teachers, counsellors and coaches;
- third parties providing services to the School, including, but not limited to, bus/transportation services and 'cloud'-based service providers;
- recipients of School publications, such as newsletters, magazines and the Yearbook;
- parents;
- anyone to whom an individual authorises the School to disclose information;
- anyone to whom we are required to disclose the information by law.

Sending information overseas

Personal information about an individual may be sent to overseas recipients, for instance, when staff or students utilise digital tools to conduct on-line surveys, when storing personal information with 'cloud' service providers that are situated outside Australia, or to facilitate a school exchange.

However, the School will not directly disclose personal information about an individual to an overseas recipient without:

- obtaining the consent of the individual (or, in the case of a student, the student's parents), which in some cases may be implied; and
- otherwise complying with the APPs.

Treatment of sensitive information

Sensitive information will be used and disclosed only for the primary purpose for which it was provided or a directly related secondary purpose.

Sensitive information may be used and disclosed for other purposes if the person to whom the information relates (or, in the case of a student, the student's parents) agrees otherwise, or the use or disclosure of the sensitive information is required or allowed by law.

3. Management and security of personal information

School staff members are required to respect the confidentiality of personal information and the privacy of individuals.

Through the use of various methods, including locked storage of paper records, data encryption and password access rights to computerised records, the School takes active steps to protect the personal information it holds from misuse, interference, loss and unauthorised access, modification or disclosure.

4. Access and correction of personal information

Under the APPs an individual has the right to obtain access to any personal information that the School holds about them, and to advise the School of any perceived inaccuracy and request correction.

The School will respond to all requests for access or correction within a reasonable time, and will give access to the information in the manner requested by the individual if it is reasonable and practicable to do so.

Students will generally be able to access and update their personal information through their parents, but older students may seek access and request corrections themselves. Requests to access or update any personal information the School holds about an individual should be made by the individual (or, in the case of a student, their parents) to Principal in writing. The School may require an individual to verify their identity and specify what information is required.

There are some exceptions to the access rights set out in the APPs. There may be circumstances where these exceptions apply, and access to personal information may not be allowed. Such circumstances include where release of the information might have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to an individual. If the School cannot provide an individual with access to personal information as requested, the School will provide a written explanation of the reasons.

The School may charge a reasonable fee to cover the cost of verifying an application for access and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

Consent and rights of access to the personal information of students

The School respects every parent's right to make decisions concerning their child's education.

Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The School 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.

Parents may seek access to personal information held by the School about them or their child by contacting the Principal or the Business Director in writing. However, there may 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, where the disclosure may result in a breach of the School's duty of care to the student, or where students have provided information in confidence.

The School may, at its discretion, on the request of a student grant that student access to personal information held by the School 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 this.

5. Disposal of Information

Scotch College retains personal information for the length of time as prescribed in the ACT. When personal information is no longer necessary for Scotch College's education and business functions, and it is lawful to do so, the College will destroy the information.

Notifiable data breaches

A data breach occurs when personal information is lost or subject to unauthorised access, modification, disclosure, or other misuse or interference. A data breach may be intentional or unintentional.

Examples of a data breach which may meet the definition of an eligible data breach under the Privacy Act include when:

- a device (such as a laptop) containing a member of the school community's personal information is lost or stolen;
- a database containing personal information is hacked; or
- personal information is mistakenly provided to the wrong person.

The Privacy Act only requires notification when an 'eligible data breach' occurs, and this policy relates only to eligible data breaches as defined by the Privacy Act. A data breach will not be an eligible data breach unless the data breach is likely to cause serious harm to an individual to whom the information relates.

Where the School suspects that an eligible data breach may have occurred, the School will carry out a reasonable and prompt assessment of whether there are reasonable grounds to believe that an eligible data breach has occurred.

If, based on that assessment, there are reasonable grounds to believe that an eligible data breach has occurred, the School will:

- immediately take appropriate steps, decided on a case-by-case basis, to contain the breach and prevent further breaches;
- prepare an eligible data breach statement as prescribed under the Privacy Act, and submit the statement to the Office of the Australian Information Commissioner (OAIC);
- notify individuals to whom the relevant information relates or who are at risk from the breach either:
    - directly, by taking such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals; or
    - if that is not possible, by publishing the contents of the statement to OAIC about the breach on the School's website and taking reasonable steps to publicise the contents of the statement; and
- review the incident and consider action to prevent future breaches.

Enquiries and complaints

If you would like further information about the way the School manages the personal information it holds, or wish to complain that you believe that the School may have breached the Australian Privacy Principles, please contact the Principal in writing.

The School will investigate any complaint and will notify you of a decision in relation to your complaint as soon as is practicable.

Who is responsible for managing data and how do they do it?

Lines of management

The Principal is responsible for ensuring all aspects of the Privacy Policy are carried out.

The Senior Leadership Team supports the Principal and also ensure that colleagues in their line of management are carrying through their relevant tasks with regard to privacy.

Middle Leaders must ensure that not only they, but those who work under them carry through the principles of the Privacy Policy.

Teaching and non-teaching staff as well as volunteers must carry through the responsibilities listed below under `What does this mean for me'.

Specific roles and how they are carried out

Certain colleagues have prominent roles in managing the collection, storage, use and disposal of data and the attendant needs for privacy. These are:

Data Manager: ICT Systems Administrator

Collection of data:

Domain	Data Owner
Students, parents	Director of Admissions
Employees, unsuccessful job applicants, contractors and volunteers with no previous link to the College	Director of People and Culture
Newly discovered former students, former parents and donors	Head of Community

Use and Storage of data:

Domain	Data Owner
Staff Administrative (e.g. staff details)	Director of People and Culture
Student Administrative (e.g. student details)	Director of Admissions

Student Pastoral	Head of relevant School/Campus
College Financial	Chief Operating Officer
Curriculum	Director of Teaching and Learning
Community e.g. former students, parents	Head of Community
Marketing	Head of Community
College Corporate e.g. Employees, unsuccessful job applicants, contractors and volunteers with no previous link to the College	Director of People and Culture
College System	Director of Information and Innovation

Disposal of data:

Domain	Data Owner
Students, parents	Director of Admissions
Employees and new volunteers	Director of People and Culture
Newly discovered former students, parents and donors	Head of Community
Hard copy of data	All staff

Scotch College Data Management Principles

Scotch College has a variety of data systems into which staff have varying levels of access, depending on their roles. The quality, privacy and security of data is critical to the College and it is therefore vital that all parties understand their roles and responsibilities as they relate to College data.

Definitions

- **Data Domain** is a collection of data that relates to a particular function within the College
- **Data Roles:**
    - **Data Manager** has a high level of technical expertise and operational responsibilities for supporting members of all Data Roles with day-to-day data administrative activities
    - **Data Owner** is a senior member of a department with ownership and responsibility for one or more Data Domains
    - **Data Administrator** is a staff member with some technical expertise and typically higher level of access than a Data User
    - **Data User** is any staff or authorized agent who accesses, inputs, amends, deletes, extracts and analyses data in order to carry out their day-to-day duties. Data Users are responsible for maintaining the quality and security of any data they access.

Principles

- The Data Owner with assistance from the Data Manager is responsible for determining what level of access is granted to roles within their responsible area.

- The Data Owner with assistance from the Data Manager is responsible for ensuring Data Administrators and Users in their responsible area have the required level of skill and training to effectively perform their role
- If personal data does not have a relevant college purpose, it should not be collected
- Each Data Domain should have a Data Administrator who takes on some of the technical responsibility and leadership for managing the data in their responsible area
- Data Users must ensure appropriate procedures are followed to uphold the quality and integrity of the data they access.
- Extraction, manipulation and reporting of data must be done only to perform College business:
    - College data should not be accessed for personal, non-college related business or other unauthorised reasons
    - Where appropriate, before any data (other than publicly available data) is used or shared outside the College, the Data Manager should be consulted
- Data stored in an electronic format must be protected by appropriate electronic safeguards and/or physical access controls that restrict access only to authorized user(s) – see Security Protocols. Similarly, data in hard copy format must also be stored in a manner that will restrict access only to authorized user(s).
- Appropriate data security measures must be adhered to at all times to assure the safety, quality and integrity of College data.
- Data shall be retained and disposed of in an appropriate manner in accordance with the College's *Records and Archives Policy*.

Security Protocols

- Members of all Data Roles must:
    - Have multi-factor authentication set up for all accounts used to access College Data (when the system supports it).
    - Never share their credentials for any College systems with an unauthorized user
        - This includes protecting credentials and systems from family members when working from home
- User passwords:
    - Protect their passwords with a password manager
    - Must be secure passwords of an appropriate length
    - Must be unique to each system (unless the system supports single sign-on)
    - At the client login screen, the password must not be saved nor any automatic login set - the password must be entered each time on login.
- Computers used to access College data systems must be protected from non-authorised use. For example, a computer must be locked and password protected whenever it is unattended or out of sight.

Complying with Australian Privacy Principles

For employees and volunteers

What does this mean for me?

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Scotch College will provide training to all employees to help them understand their responsibilities when handling data.
- Strong passwords must be used and they should never be shared.
- Personal and sensitive data should not be disclosed to unauthorised people, either within the company or externally. In the event that personal data needs to be sent externally, it must not be sent by unencrypted email. Techniques for sending personal and sensitive data can be obtained from the College's IT Support.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from the IT Department if they are unsure about any aspect of data protection.

When the system fails and we have a data breach, please note:

1. **Immediate actions for the first person to discover the breach:**

- Immediately report to the appropriate person/people
- Do not destroy any evidence that might be needed to investigate
- Assist with the investigation and documentation as required

2. **Thereafter, the data breach action plan (see separate document) will be followed by the appropriate leaders.**

Otherwise, in your day to day work, please note the following based on your position in the College

I am a Teacher:

I may have access to the following data:	It is in the following format:	I access this data in the following way:
• Student records • Student communications (emails, letters) • Parent/guardian records • Parent/guardian communications • Details of next of kin • Staff communications • Some staff personal data	• Electronic: Synergetic, SEQTA, Care Monkey, email system • Hard copy: letters, written notes, printed copies	• Through my laptop, phone, tablet • In a file, in a filing cabinet

Key questions for you:

Collection	Usage	Storage	Disposal
If you collected the data, did you: • Tell the sender what you are collecting it for, including next of kin? • Tell the sender that you operate by the Australian Privacy Principles, enshrined in the Scotch	If you use this data: • Do you only use it for its primary or secondary purpose? • Are you aware of what you must do if you are NOT using this for its primary or secondary purpose?	If you store data electronically: • Have you secured access so that no-one else but you can access it? • Encrypted and password protected your machines and devices? • Set your screen to immediately lock and	Are you aware that you must dispose of data when it has outlived its purposes? • Do you know how long you must keep this data? • Do you have secure way of disposing of this data?

College Privacy Policy? • Collect any data including pictures, moving images etc.. on any personal device? If so: ○ Have you gained permission to do that? ○ Have you moved it to a school owned platform? ○ Have you deleted this data from your own device?	• Do you always seek to be respectful of the data you are given by anyone in a professional capacity?	require a password whenever you leave your machine unattended? • Have File Vault or Bitlocker on so your hard disk is protected? • Have encryption on your external hard drive? If you store data in hard copy: • Are all methods of storage locked at all times when you are away from your work area? • If your methods of storage are shared with others, do you have an agreed lock-up process? • **DO YOU KNOW WHAT TO DO IF THERE IS A DATA BREACH? (See appendix to this document)**	

I am a Non-Teacher:

I may have access to the following data:	It is in the following format:	I access this data in the following way:
• Student records • Student communications (emails, letters) • Parent/guardian records • Parent/guardian communications • Details of next of kin • Staff communications • Some staff personal data • Information from prospective parents • Data from previous parents • Data from Old Collegians • Data from contractors and consultants • Data from unsuccessful applicants for roles • Data from volunteers	• Electronic: Synergetic, SEQTA, Care Monkey, email system • Hard copy: letters, written notes, printed copies	• Through my laptop, phone, tablet • In a file, in a filing cabinet

Key questions for you:

Collection	Usage	Storage	Disposal
If you collected the data, did you:	If you use this data:	If you store data electronically:	Are you aware that you must dispose of

• Tell the sender what you are collecting it for, including next of kin?
 	
• Tell the sender that you operate by the Australian Privacy Principles, enshrined in the Scotch College Privacy Policy?
• Collect any data including pictures, moving images etc.. on any personal device? If so:
  ○ Have you gained permission to do that?
  ○ Have you moved it to a school owned platform?
  ○ Have you deleted this data from your own device?
	• Do you only use it for its primary or secondary purpose?
	• Are you aware of what you must do if you are NOT using this for its primary or secondary purpose?
	• Do you always seek to be respectful of the data you are given by anyone in a professional capacity?
		• Have you secured access so that no-one else but you can access it?
		• Encrypted and password protected your machines and devices?
		• Set your screen to immediately lock and require a password whenever you leave your machine unattended?
		• Have File Vault or Bitlocker on so your hard disk is protected?
		• Have encryption on your external hard drive
		
		If you store data in hard copy:
		
		• Are all methods of storage locked at all times when you are away from your work area?
		• If your methods of storage are shared with
			data when it has outlived its purposes?
			
			• Do you know how long you must keep this data?
			• Do you have secure way of disposing of this data?

		others, do you have an agreed lock-up process? • **DO YOU KNOW WHAT TO DO IF THERE IS A DATA BREACH? (See appendix to this document)**	

I am a Council or Committee Member, Volunteer or involved with the College in a non-paid capacity

I may have access to the following data:	It is in the following format:	I access this data in the following way:
• Confidential corporate data • Student records • Student communications (emails, letters) • Parent/guardian records • Parent/guardian communications • Details of next of kin • Staff communications • Some staff personal data • Data from other volunteers	• Electronic: Synergetic, SEQTA, Care Monkey, email system • Hard copy: letters, written notes, printed copies	• Through my laptop, phone, tablet • In a file, in a filing cabinet • Through any method of storage used by the employees I am working with

Key questions for you:

Collection	Usage	Storage	Disposal
If you collected the data, did you:	If you use this data:	If you store data electronically:	Are you aware that you must dispose of

• Tell the sender what you are collecting it for, including next of kin?
 	
• Tell the sender that you operate by the Australian Privacy Principles, enshrined in the Scotch College Privacy Policy?
• Collect any data including pictures, moving images etc.. on any personal device? If so:
  ○ Have you gained permission to do that?
  ○ Have you moved it to a school owned platform?
  ○ Have you deleted this data from your own device?
	• Do you only use it for its primary or secondary purpose?
	• Are you aware of what you must do if you are NOT using this for its primary or secondary purpose?
	• Do you always seek to be respectful of the data you are given by anyone in a professional capacity?
		• Have you secured access so that no-one else but you can access it?
		• Encrypted and password protected your machines and devices?
		• Set your screen to immediately lock and require a password whenever you leave your machine unattended?
		• Have File Vault or Bitlocker on so your hard disk is protected?
		• Have encryption on your external hard drive
		
		If you store data in hard copy:
		
		• Are all methods of storage locked at all times when you are away from your work area?
		• If your methods of storage are
			data when it has outlived its purposes?
			
			• Do you know how long you must keep this data?
			• Do you have secure way of disposing of this data?

		shared with others, do you have an agreed lock-up process? • **DO YOU KNOW WHAT TO DO IF THERE IS A DATA BREACH? (See appendix to this document)**	

I am a Middle Leader - Key questions for you:

- Are you checking, periodically, the principles in this policy and the practices above with your teams?
- Are you feeding back questions and comments to the Senior Leadership Team about this policy?
- **DO YOU KNOW WHAT TO DO IF THERE IS A DATA BREACH? (See separate documents)**

I am a Senior Leader - Key questions for you:

- Do you periodically check:
  - This policy?
  - The record of expected practices and behaviours above?
  - By cross-referencing these documents with the Risk documentation?

  - The work of those in your line management so they are following these instructions?
  - That you are reporting and managing concerns or weaknesses?
  - Communications and culture around compliance?

  - On the integrity and security of our storage systems?
  - That the data breach protocols are still right?
  - That disaster recovery protections are in place?
  - That we understand as best as possible the increasingly complex ways in which we may be vulnerable to hacking and cyber-attack?

- **DO YOU KNOW WHAT TO DO IF THERE IS A DATA BREACH? (See separate documents)**