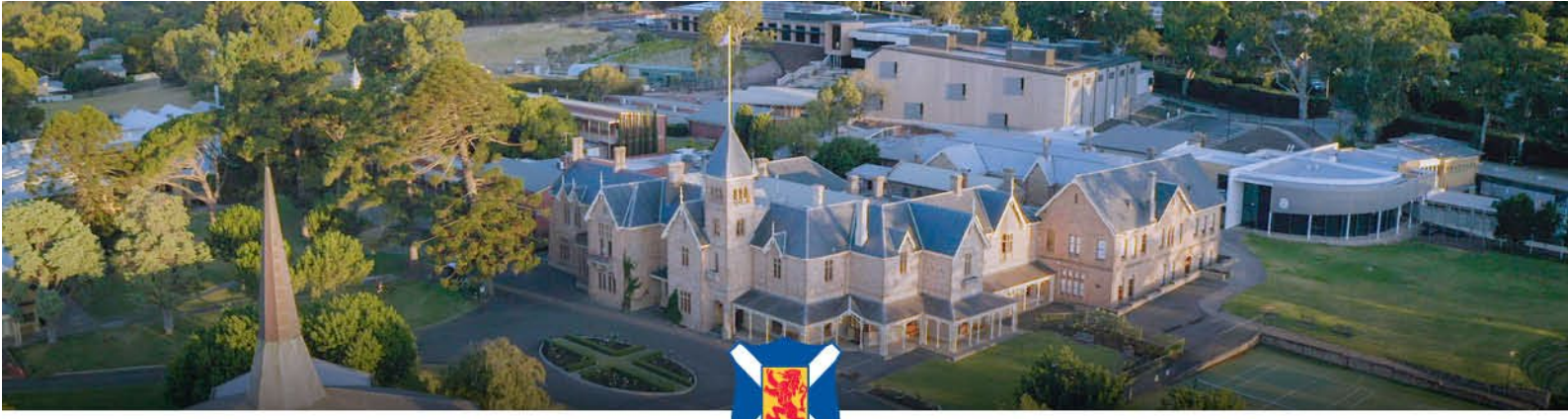


Privacy Policy

Version History

Version No.	Description of Changes	Effective Date
V2.0	Revised Policy through 2023/2024 policy rationalisation and update process.	28/08/2024

1 Purpose

This policy outlines how Scotch College uses and manages Personal Information.

The College is bound by the Australian Privacy Principles contained in the Privacy Act 1988 (Commonwealth) and will collect, use and retain Personal Information in accordance with those Principles.

2 Scope

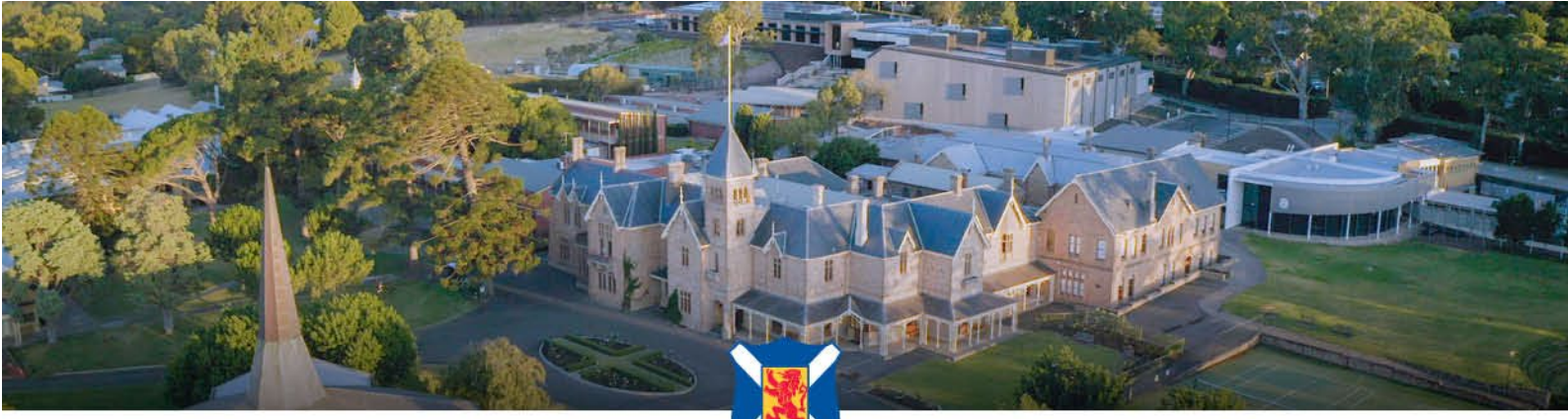
This policy applies to all current and past students, parents and guardians of students, employees, Council and Committee Members, consultants, volunteers and contractors of the College.

This policy covers the use of Personal Information of other members of the community who deal with the College.

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

3 Definitions

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 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, Health Information, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record.
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.

4 Principles

The College complies with the Australian Privacy Principles (APPs) issued by the Office of the Australian Information Commissioner (OAIC). Australian Privacy Principles | OAIC

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

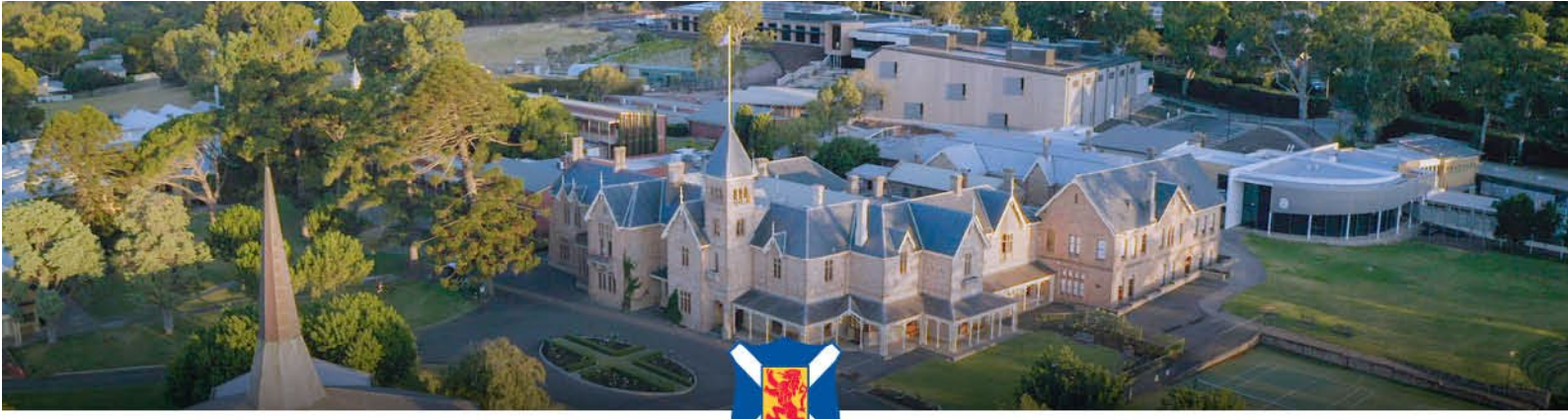
APP 8: Cross-border disclosure of personal information

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

The APPs do not apply to an employee record where the personal information is directly related to a current or former employment relationship between the College and an employee.

5 Responsibilities

The Council of Governors are responsible for ensuring the College has the appropriate structures in place to comply with the APPs issues by the OAIC.

The Principal is responsible for ensuring all aspects of this policy are carried out.

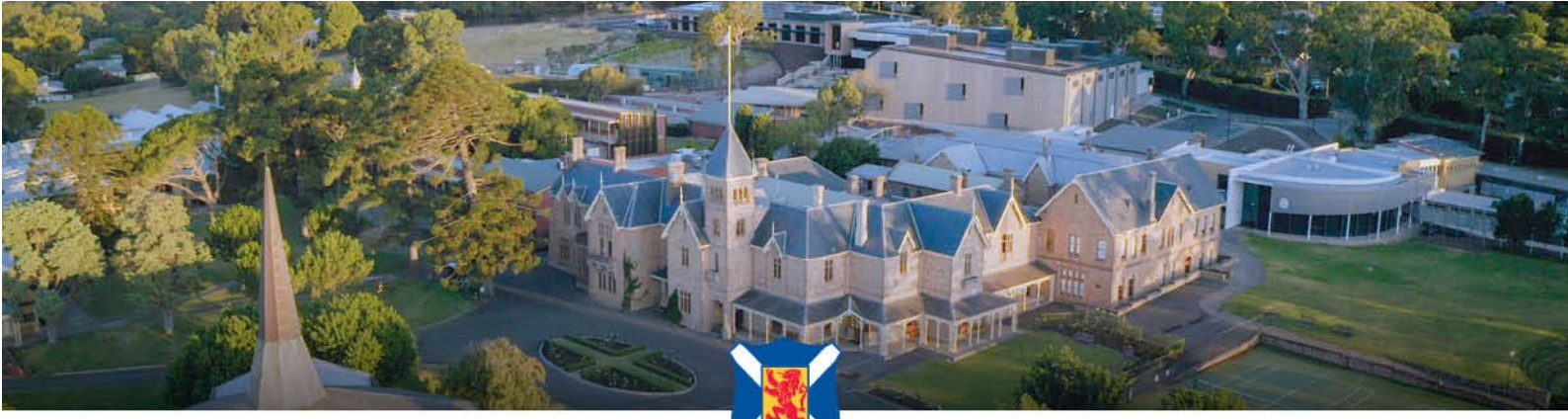
The Senior Leadership Team supports the Principal in the application of this policy and ensuring their line of management are aware of privacy requirements and activities remain in compliance with the requirements of the College, with regard to privacy.

Staff and Volunteers are responsible for making themselves aware of privacy requirements and conduct activities in compliance with the requirements of this Policy.

- The only people able to access data covered by this policy should be those who need it for their work.
- Personal Information should not be shared informally. When access to personal information is required, employees can request it from their line managers.
- The College will provide training to all employees to help them understand their responsibilities for managing personal information.
- Strong passwords must be used, and they should never be shared.
- Personal and sensitive information should not be disclosed for reasons other than those permitted under the Privacy
  Where Information 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.
- Personal Information should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and securely disposed of.
- Employees should request help from the IT Department if they are unsure about any aspect of data protection or the COO if they are unsure of their obligations with respect to personal information.

6 General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Personal Information should not be shared informally. When access to personal information is required, employees can request it from their line managers.



- The College will provide training to all employees to help them understand their responsibilities for managing personal information.
- Strong passwords must be used and they should never be shared.
- Personal and sensitive information should not be disclosed for reasons other that those permitted under the Privacy
  Where Information 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.
- Personal Information should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and securely disposed of.
- Employees should request help from the IT Department if they are unsure about any aspect of data protection or the COO if they are unsure of their obligations with respect to personal information.

7 Collection

In the conduct of its operations and obligations, the College collects and holds personal information, including health information and other sensitive information with respect to (but not limited to):

- students and parents and/or guardians, before, during and after the course of a student's enrolment at the College;
- job applicants, staff members, College Council & Committee members, other volunteers and contractors; and
- other people who come into contact with the College.

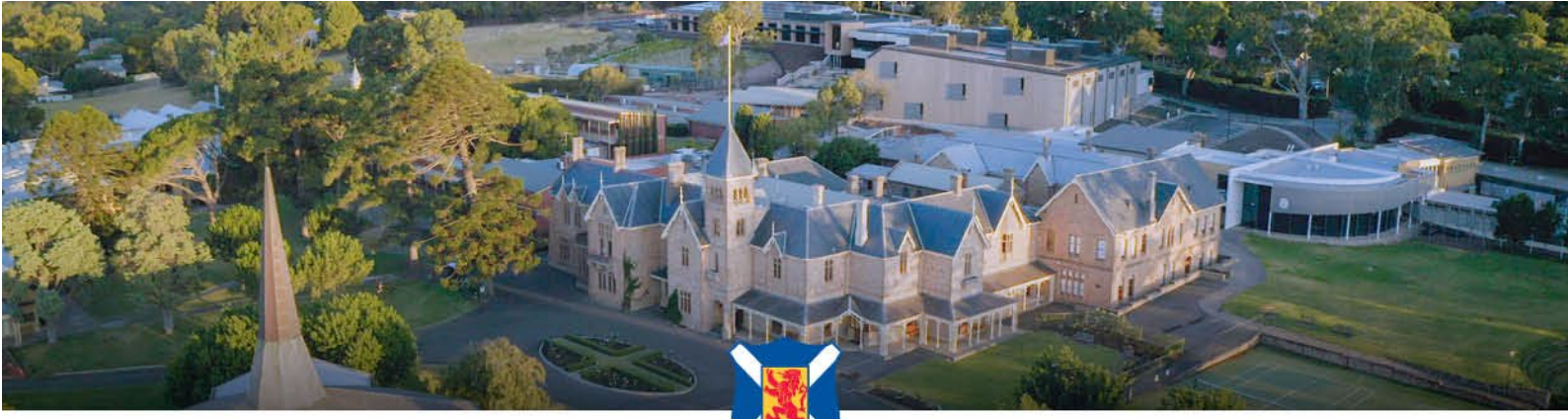
Personal Information may be:

7.1 Provided by an Individual

The College 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 and/or guardians) by way of forms (paper and/or electronic) filled out by parents or students, face-to-face meetings and interviews, on-line surveys, emails or telephone calls.

7.2 Provided by other people

In some circumstances the College may be provided with personal information about an individual from a third party. For example, the College may receive a report provided by a medical professional or an employment reference from another College.



8 Use and Disclosure of personal information by the College

From time to time, the College will use or disclose personal information it has collected for a particular purpose - ie: the purpose It was collected for. (*the primary purpose*).

The College may use or disclose personal information it has collected for other purposes (*secondary purposes*), but only where you (or, in the case of a student, the student's parents and/or guardian) consent.

The College may use or disclose personal information it has collected for a *secondary purpose*, without specific consent, if the *secondary purpose*:

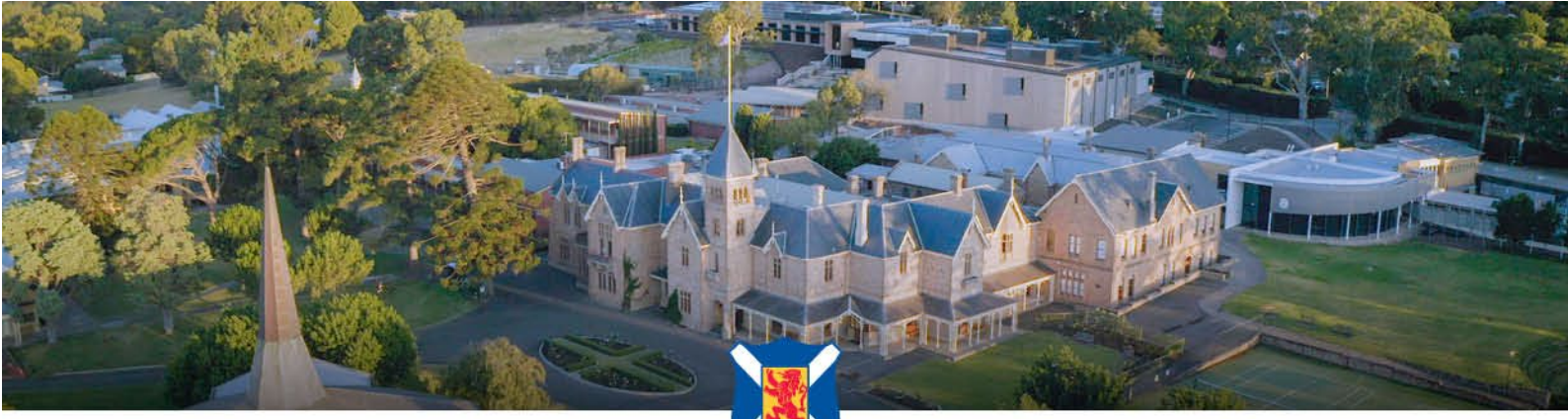
- is something you would reasonably expect;
- is required or authorised by or under an Australian law or a court/tribunal order;
- is related to the *primary purpose* (Sensitive Information must be directly related to the *primary purpose*).
- Any other reason authorised under APP 6.

For administrative and educational purposes, the College may, from time to time, disclose personal information to (but not limited to):

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

Depending on the circumstances by which Personal Information was collected, the above purposes are classified as *primary purpose* or *secondary purposes*.

8.1 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 College exchange.

However, the College 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 and/or guardian), which in some cases may be implied; and

otherwise complying with the APPs.

9 Management and security of personal information

The College respects the confidentiality of personal information and the privacy of individuals.

The College maintains an information asset register to classify and categorise types of personal information and uses this register to takes active steps to protect the personal information it holds from misuse, interference, loss and unauthorised access, modification or disclosure.

10 Access and correction of personal information

An individual has the right to obtain access to any personal information that the College holds about them, and to advise the College of any perceived inaccuracy and request correction.

The College 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.

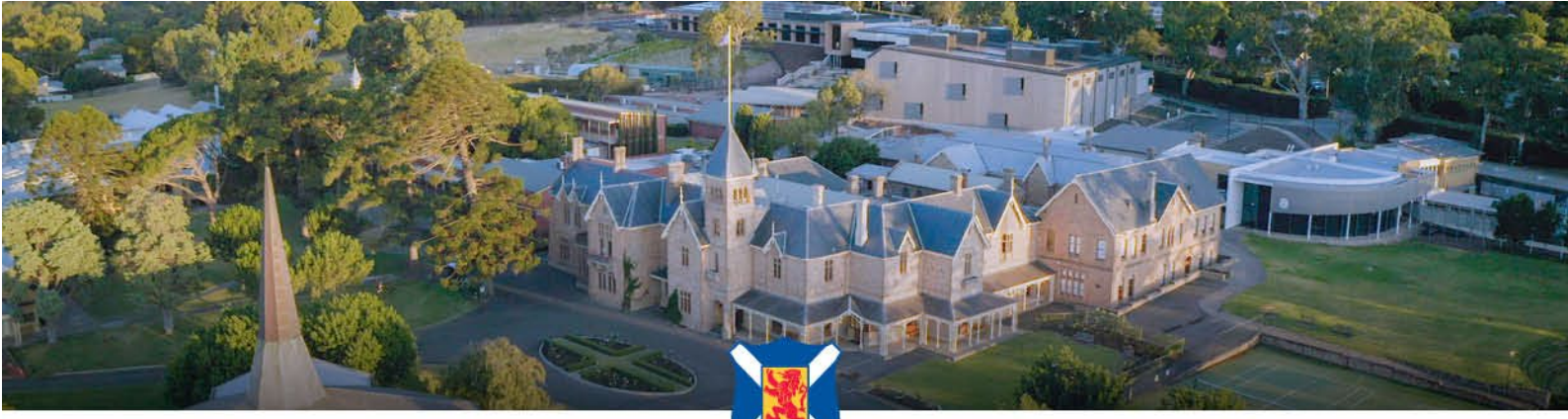
Students will generally be able to access and update their personal information through their parents and/or guardian, but older students may seek access and request corrections themselves.

Requests to access or update any personal information the College holds about an individual should be made by the individual (or, in the case of a student, their parents and/or guardian) to the Principal in writing. The College may require an individual to verify their identity and specify what information is required.

There may be circumstances where an exception may 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
- where the release may result in a breach of the College's duty of care to an individual.

If the College cannot provide an individual with access to personal information as requested, the College will provide a written explanation of the reasons.



The College 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 College will advise the likely cost in advance.

11 Consent and rights of access to the personal information of students

The College respects every parent and or guardian'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 and or guardians. 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.

Parents and/or guardians may seek access to personal information held by the College about them or their child by contacting the Principal or the Chief Operating Officer 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 College's duty of care to the student, or
- where students have provided information in confidence.

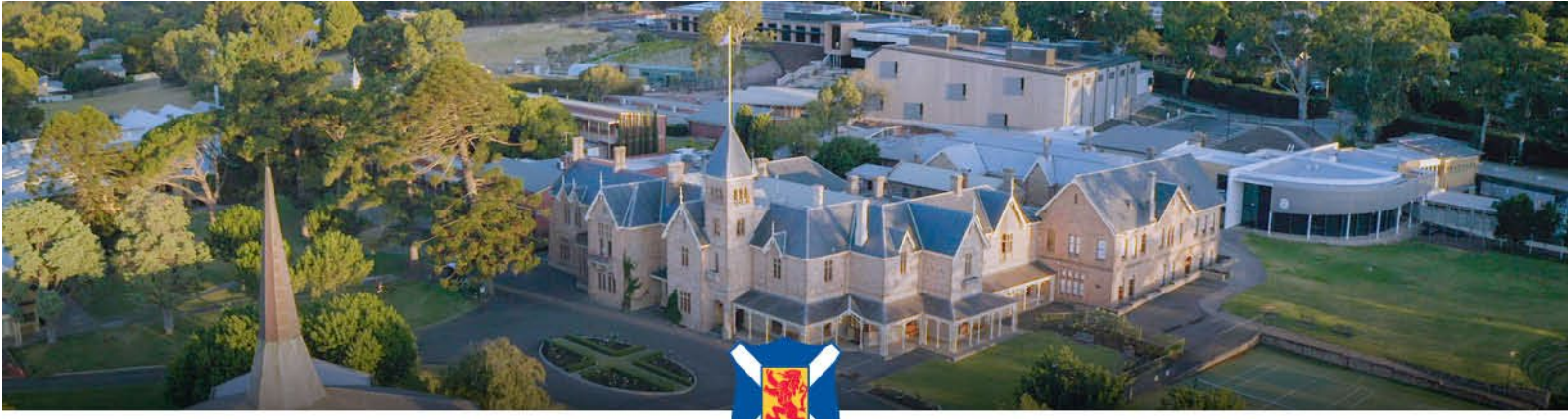
The College may, at its discretion, on the request of a student grant that student access to personal information held by the College about them or allow a student to give or withhold consent to the use of their personal information, independently of their parents and/or guardians. This would normally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

12 Disposal of personal information

Scotch College retains personal information for the length of time as prescribed in the Privacy Act 1988 and/or the recommendation from the Australian Society of Archivists Records Retention Schedule for Non-Government Schools, whichever is longer.

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 securely dispose of the information.

13 Notifiable data breaches



Data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harms to individuals and entities.

Should a data breach occur, the College will take steps to:

Contain the data breach to prevent any further compromise of personal information.

Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals.

Where practical, the College will take remedial action to limit the impact of the breach on affected individuals.

Notify individuals and the OAIC, as required by the OAIC.

Review the incident and consider what actions can be taken to prevent future breaches.

There is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis.