



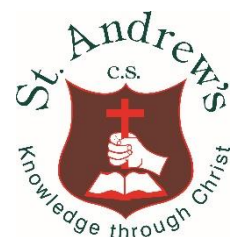
Privacy Policy

84 Washpool Road Clarenza NSW 2460

Telephone: (02) 6643 4770

Email: reception@standrewscs.nsw.edu.au

Web: www.standrewscs.nsw.edu.au



Created	Reviewed	Reviewed	Reviewed	Reviewed	Reviewed
27/08/2021	23/09/2024				

CONTENTS

Scope of Policy and Source of Obligation	3
What is personal information?	3
Kinds of personal information we collect	4
How we collect personal information.....	4
Purposes for which we collect, use and disclose personal information	5
School Counsellors	6
Exchange of Information.....	6
Who we disclose personal information to.....	7
How we store personal information.....	7
Fundraising and marketing	7
Sending and storing information overseas	8
Security of personal information	8
Access and correction of personal information.....	9
Consent and rights of access to the personal information of students.....	9
Data Breaches	10
Compliance Management.....	10
Enquiries and complaints.....	10
Primary resource and support material.....	11

Scope of Policy and Source of Obligation

In addition to the requirements of the Education Act, schools must be aware of, understand and comply with other relevant state and Commonwealth legislation. Including but not limited to the [Privacy and Personal Information Act 1998](#).

This Privacy Policy sets out how St. Andrew's Christian School ('the School') manages personal information and rights in relation to personal information, including how to complain and how we deal with complaints.

The School is bound by the [Australian Privacy Principles](#) (APP) contained in the Commonwealth Privacy Act 1988 (Privacy Act). In relation to health records, the School is also bound by the Health Privacy Principles which are contained in the Health Records and Information Privacy Act 2002 (NSW).

Under the Privacy Act and the Health Records Act, the Australian Privacy Principles and Health Privacy Principles do not apply to certain treatment of an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record held by the School, where the treatment is directly related to a current or former employment relationship between the School and the employee.

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

The current version of this Privacy Policy is published on our website.

APP 1 Open and transparent management of personal information

The School is required to ensure that personal information is managed in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 Anonymity and pseudonymity

The School is required to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

What is personal information?

Personal information includes general information about a person, but also includes "sensitive information" and "health information".

Personal information can include a person's name, address, some financial information, marital status, family information such as next of kin, phone numbers and limited information as to work status and location.

Sensitive information includes information relating to racial or ethnic origin, political opinions or political affiliations, philosophical or religious beliefs or affiliations, membership of professional or trade associations or trade unions, sexual identification or practices, criminal records and health and genetic information.

Health information includes any information collected about an individual's health or disability and any information collected in relation to a health service that is provided. It can include such things as diagnoses and treatments, identified symptoms, notes or reports from medical professionals and prescriptions.

Kinds of personal information we collect

The types of information the School collects includes (but is not limited to) personal information, including health and other sensitive information, about:

- ▶ students and parents and/or guardians ('Parents') before, during and after the course of a student's enrolment at the School, including:
 - name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;
 - parents' education, occupation, language spoken at home, nationality and country of birth;
 - health information (e.g., details of disability and/or allergies, dietary requirements, absence notes, immunisation details, medical reports and names of doctors);
 - results of assignments, tests and examinations;
 - conduct and complaint records, or other behaviour notes, and school reports;
 - information about referrals to government welfare agencies;
 - counselling reports;
 - health fund details and Medicare number;
 - any Family Court orders;
 - criminal records;
 - volunteering information; and
 - photos and videos at School events.

- ▶ job applicants, volunteers and contractors, including:
 - 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;
 - health information (e.g., details of disability and/or allergies, and medical certificates);
 - complaint records and investigation reports;
 - leave details;
 - photos and videos at School events;
 - workplace surveillance information; and
 - work emails and private emails (when using work email address) and Internet browsing history; and

- ▶ other people who come into contact with the School, including name and contact details and any other information necessary for the particular contact with the School.

How we collect personal information

APP 3 Collection of solicited personal information

This APP outlines when the School can collect personal information that is solicited. Higher standards are applied to the collection of 'sensitive' information.

APP 4 Dealing with unsolicited personal information

This APP outlines how the School must deal with unsolicited personal information.

APP 5 Notification of the collection of personal information

This APP outlines when and in what circumstances the School must notify an individual of certain matters in relation to personal information that it collects.

Personal information you provide: The School generally collects personal information about an individual directly from the individual (or their Parent in the case of students). This includes by way of forms, face-to-face meetings and interviews, 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 a report provided by a medical professional, a reference from another school or a referee for a job applicant. If a student transfers to a new school, the new school may collect personal information about the student from the student's previous school to facilitate the transfer of the student.

Information given by consent: Most personal information, especially that of a sensitive nature, can only be collected by the School with the consent of the individual involved. However, where consent for requested information is refused, and such information may prevent the School from discharging its duty of care to the entire school body (students, parents, family, staff, volunteers, contractors etc.), the School may not be able to enrol or continue the enrolment of the student. This also applies to applications for staff vacancies, volunteer positions and contract services.

Personal information from other sources: The School maintains systems of surveillance, including CCTV or monitoring of computer systems, networks and facilities. We may collect personal information through activities (such as CCTV security cameras) and student ICT use monitoring.

People interacting with the School or using those systems will be advised using School policies, notices and signs in areas that they may be monitored, thus collecting personal information. The [Student ICT Use Agreement](#) outlines this. Consent to this monitoring is given implicitly on employment or as part of worker contracts.

Purposes for which we collect, use and disclose personal information

The purposes for which the School collects, uses and discloses personal information depend on the relationship and include the following:

Students and Parents:

- providing schooling and school activities;
- satisfying the needs of Parents, the needs of students and the needs of the School throughout the whole period a student is enrolled at the School;
- making required reports to government authorities;
- keeping Parents informed about matters related to their child's schooling, through correspondence, apps, newsletters and magazines;
- day-to-day administration of the School;
- looking after students' educational, social and health wellbeing;
- seeking donations for the School (see the 'Fundraising and Marketing' section of this Privacy Policy); and
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

Volunteers:

- make contact about, and administer, the volunteer position;
- for insurance purposes; and
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

Job applicants and contractors:

- assessing and (if successful) engaging the applicant or contractor;
- administering the individual's employment or contract;
- for insurance purposes; and
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

School Counsellors

When considering whether they should disclose a student's personal information, school counsellors must consider relevant privacy laws and their duty of care to the student and the student's own views about whether they want their information to be shared.

STACS will ensure that:

- Students are made aware at the outset of conversations with the School Counsellor the situations when their information may be disclosed to other parties, such as the school, parents or police;
- The School communicates its privacy and communications policies to the school community, including in relation to the disclosure of personal information;
- The School Counsellor has sufficient training in their obligations, including when it is appropriate to disclose information;
- Counselling records (considered sensitive health information) are securely stored and appropriately disposed according to School requirements.

Please refer to the [Student Counselling Services Policy and Procedures](#) for more details about the privacy obligations of School Counsellors.

Exchange of Information

The Children and Young Persons (Care and Protection) Act facilitates the exchange of information between the agencies that have responsibilities relating to the safety, welfare or well-being of children and young persons.

Students

Schools are permitted to request information relating to the safety, welfare or well-being of a child or children in order to assist the school or other prescribed body to:

- a. Make a decision, assessment or plan; or
- b. Initiate or conduct any investigation; or
- c. Provide any service relating to the safety, welfare or well-being of a child or children;
- d. Manage any risk to a child or class of children.

If a school receives a request for information under the legislation, it must comply with the request if the school reasonably believes that the information may assist the requesting agency or school.

The legislation specifically provides that it takes precedent over any other act or law that prohibits or restricts the disclosure of information, including the Privacy Act and any confidentiality undertakings (for example, Deeds of Release) or an individual's privacy. The only exemption would relate to a situation that endangered a child's safety.

Employees

Under the legislation described above, schools may provide information about former staff members, or request information relating to applications for employment.

If a school employee leaves (whether by dismissal or resignation), and the school reasonably believes that the employee may have harmed the safety, welfare or well-being of any children, any confidentiality agreement or Deed of Release that the school and an employee may enter into prohibiting the disclosure of the circumstances of the employee's termination will not have effect.

Where the school provides information in good faith under the Act, it cannot be liable for any civil or criminal action, or be in breach of any code of conduct or professional ethics.

Who we disclose personal information to

APP 6 Use or disclosure of personal information

This APP outlines the circumstances in which the school may use or disclose personal information that it holds.

The School may disclose personal information, including sensitive information, for educational, care and administrative purposes, and to seek support and advice. This may include to:

- other schools and teachers at those schools, including a new school to which a student transfers to facilitate the transfer of the student;
- government departments (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the School, including specialist visiting teachers, coaches, volunteers, and counsellors;
- organisations that assist us with fundraising
- providers of specialist advisory services and assistance to the School, including in the area of Human Resources, child protection, students with additional needs and for the purpose of administering Apps for education and ensuring its proper use (see further the section below 'Sending and storing information overseas');
- providers of learning and assessment tools;
- assessment and educational authorities, including the NSW Education Standards Authority 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);
- agencies and organisations to whom we are required to disclose personal information for education, funding and research purposes;
- people providing administrative and financial services to the School; the provider of our information management and storage system and other information technology services; recipients of School publications, such as newsletters and magazines;
- students' parents or guardians;
- anyone you authorise the School to disclose information to; and
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

How we store personal information

We store your personal information in hard copy and electronically. We use information management and storage systems provided by third party service providers. Personal information is stored with and accessible by the third party service providers for the purpose of providing services to the School in connection with the systems.

Fundraising and marketing

APP 7 Direct marketing

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

The School treats seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to provide a quality learning environment in which both students and staff thrive. Your personal information may be used to make an appeal to you.

It may also be disclosed to organisations that assist in the School's fundraising activities, for example, external fundraising organisations.

If you do not want to receive fundraising communications from us, please notify the Principal.

Sending and storing information overseas

APP 8 Cross-border disclosure of personal information

This APP outlines the steps the School must take to protect personal information before it is disclosed overseas.

The School may disclose personal information about an individual to overseas recipients in certain circumstances, for instance, to facilitate a school exchange.

The School may use online or 'cloud' service providers to store personal information and to provide services to the School 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 and provide technical support. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

An example of such a cloud service provider is Microsoft Office 365. Microsoft provides service, and stores and processes limited personal information for this purpose. School personnel and the Association of Independent Schools NSW and its service providers may have the ability to access, monitor, use or disclose emails, communications (e.g., instant messaging), documents and associated administrative data for the purposes of administering Office 365 and ensuring its proper use.

Security of personal information

APP 9 Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 Quality of personal information

The School must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. It must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 Security of personal information

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

The School has in place steps to protect the personal information the School holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

These steps include:

- Restricting access to information on the School databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile.
- Ensuring all staff are aware that they are not to reveal or share personal passwords.
- Ensuring where personal and health information is stored in hard copy files that these files are stored in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need to know basis.
- Implementing physical security measures around the School buildings and grounds to prevent break-ins.

- Implementing ICT security systems, policies and procedures, designed to protect personal information storage on our computer networks.
- Implementing human recourse policies and procedures, such as email and internet usage, confidentiality and document security policies, designed to ensure that staff follow correct protocols when handling personal information.
- Undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime;
- Using a student code: student initials, current grade, calendar year. For example Walter Melon is in Grade 9 in 2024 – WM0924

Access and correction of personal information

APP 12 Access to personal information

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

APP 13 Correction of personal information

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

Under the Commonwealth Privacy Act and the Health Records Act, an individual has the right to seek access to, and/or correction of, any personal information which the School holds about them.

Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access, update or correct any personal information the School holds about you or your child, please contact the Principal by email, post or telephone at principal@standrewscs.nsw.edu.au or 02 66434770.

The School may require you to verify your identity and specify what information you require. If the information sought is extensive, the School may charge a reasonable fee for giving access to your personal information (but will not charge for the making of the request or to correct your personal information). The School will advise the likely cost in advance.

If we decide to refuse your request, we will provide you with written notice explaining the reasons for refusal (unless, in light of the grounds for refusing, it would be unreasonable to provide reasons) and how to complain.

Parents can also log on to the Engage Parent Portal and correct and update some of their or their child's personal information at any time.

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. Generally, 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 - details in the section above 'Access and correction of personal information'.

There may be occasions when access is denied. Such occasions may include (but are not limited to) where the School believes the student has capacity to consent and the School is not permitted to disclose the information to the Parent without the student's consent, 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 School's duty of care to the student.

The School may, at its discretion, on the request of a student grant that student access to 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 it.

In all cases, we will follow any Court Orders in place. If there are no Court Orders, we will contact either parent.

Data Breaches

Refer to our Data Breach Policy.

Compliance Management

Business Manager

The School's Business Manager or delegate

- a. is responsible for ensuring each individual is aware of the need to collect information
- b. is responsible for collection and maintenance of all privacy related issues
- c. will conduct periodic reviews of information handling practices and security procedures to ensure the School complies with the APPs, including identifying and managing privacy risks, compliance issues
- d. will manage inquiries or complaints from individuals about its compliance with the APPs
- e. will make this Privacy Policy available in an accessible form to anyone who asks for it

Staff Training

Achievement and continued compliance with the Privacy Act will be through the conduct of the School's employees. The School has in place comprehensive confidentiality and security procedures and provide training to all individuals who have access to personal information as to the appropriate manner in which personal information should be treated.

School's staff members will be trained and made aware of the principles of the Privacy Act through:

- a. having the Privacy Policy available to all staff on the PolicyConnect landing page;
- b. informing staff of the requirements of confidentiality and extending this obligation contractually where necessary;
- c. completion of the training module "[Privacy in Practice](#)" provided by the federal government's Office of the Australian Information Commissioner;
- d. holding internal briefings and workshops.

Enquiries and complaints

The School will advise individuals of the Privacy Policy and how they may complain about a breach of the Australian Privacy Principles. The School will deal with that complaint in line with the steps in our [Complaints and Grievances Policy](#).

The School will advise individuals in their collection statements that Privacy Policy contains this information.

Complaints of Privacy breaches should be directed in the first instance to the School. If the complaint is unable to be resolved at the School level, the Information Commissioner may investigate the complaint. A complaint that is upheld may be resolved by an order that the school redress any loss or damage to the person whose privacy has been breached.

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 has breached the Australian Privacy Principles or the Health Privacy Principles please contact the Principal] by email, post or telephone at principal@standrewscs.nsw.edu.au or 02 66434770 or 84 Washpool Road Clarenza NSW 2460

The School will investigate any complaint and will notify in relation to your complaint as soon as is practicable after investigation and a decision has been made.

If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (OAIC) via the OAIC website, www.oaic.gov.au.

Primary resource and support material

Privacy Compliance Manual, April 2023 - A manual for schools that are members of an association of Independent schools and schools and systems that are represented by the National Catholic Education Commission.

Link: Accessed 23-9-24 [Privacy Compliance Manual](#)

Within the Manual are a range of Templates:

- privacy planning templates (student; parent)
- permission to share personal information (including photos/videos) for promotional and other purposes
- short form disclosure statement to students
- short form disclosure statement to students alternative (sample script for counsellors)

Within the Manual are a range of Sample Collection Notices

- Sample Standard Collection Notice
- Employment Collection Notice (for job applicants)
- Contractor Collection Notice