PRIVACY POLICY

INTRODUCTION

This Privacy Policy sets out how Southern Vales Christian College manages personal information provided to or collected by it. Reviews and updates take place from time to time when there are new laws and technology, changes to the College's operations and practices as well as to make sure it remains appropriate to the changing College environment.

The College is bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act 1988.

Students and parents and/or guardians and caregivers ('parents')

In relation to personal information of students and parents, the College's primary purpose of collection is to enable the College to provide an education for the student. This includes satisfying the needs of parents, the needs of the student and the needs of the College throughout the whole period the student is enrolled at the College.

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

- Looking after students' educational, social and medical wellbeing;
- Day to day administration of the College including the collection of school tuition fees;
- To keep parents informed about matters related to their child's Schooling, through correspondence, newsletters and magazines;
- Seeking donations and marketing for the College; and
- To satisfy the College's legal obligations and allow the College to discharge its duty of care.

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

What kinds of personal information does the College collect?

The College collects information to provide a safe learning environment for students. It therefore collects all relevant information, including (but not limited to):

- Health information
- Custody information
- Contact details
- Academic records
- Behavioural records
- Bank details

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

- Students and parents before, during and after the course of a student's enrolment at the College;

The College obtains information generally through:

- Paper forms completed by parents/caregivers
- Face to face interviews and phone calls
- Electronic correspondence through email
- Online forms through the College's website
- Reports from professionals
- Reference from previous school or childcare
- Platforms including SEQTA and Class DOJO

Personal information provided by 'Parents' and students

The College will generally collect personal information held about an individual by way of forms filled out by parents or students, face-to-face meetings and interviews, emails and telephone calls. On occasions, people other than parents and students provide personal information.

Personal information provided by others

In some circumstances the College may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or reference from another College or a referee statement from a nominated giver to the College by the enrolling parent/caregiver.

.

How will the college use the personal information provided

The College will use personal information it collects for the primary purpose of collection as described below, and for such other secondary purposes that are related to the primary purpose of collection and reasonable expectations, or to which have been consented.

Advisory and Other Purposes
The College may, from time to time, disclose personally identifiable information to others for advisory, administrative, child protection, legal or educational purposes. Such disclosures will only be in relation to the primary purpose of collection, or for secondary purposes, related to the primary purpose, and which the individual would reasonably expect. If the College does not receive the information referred to above, it may not be able to fulfill its obligations or engage a contractor/supplier, as the case may be.

Legally Required Releases of Information
We may be legally required to disclose your personally identifiable information. Such disclosure may be (a) required by subpoena, law, or other legal process; (b) necessary to assist law enforcement officials or government enforcement agencies; (c) necessary to investigate violations of or otherwise enforce our legal obligations; (d) necessary to protect us from legal action or claims from third parties including you; and/or (e) necessary to protect the legal rights, personal/real property, or personal safety of the College, our users, employees, and affiliates.

Third Party use of Information

The College may use contractors to assist in its functions and in doing so may be required to disclose relevant personal information to these contractors to enable them to meet their obligations. The College will take reasonable precautions to ensure that those third parties comply with the Australian Privacy Principles.

Employees -Job applicants and contractors/suppliers

In relation to personal information of job applicants and contractors/suppliers, the College's primary purpose of collection is to assess and (if successful) to engage the applicant or contractor/supplier, as the case may be.

The purposes for which the College uses personal information of job applicants and contractors/suppliers include:

- Administering the individual's engagement, as the case may be;
- For insurance purposes;
- Seeking donations and marketing for the College; and
- Satisfying the College's legal obligations, for example, in relation to child protection legislation.

Volunteers

The College also obtains personal information about volunteers who assist the College in its functions or to conduct associated activities, such as Old Scholars, extra-curricular activities, clubs or groups under the College's authority, to enable the College and its volunteers to work together.

Marketing, community relations and fundraising

The College treats marketing, community relations and events, and seeking donations for the future growth and development of the College, or for community and overseas service, as an important part of ensuring the College continues to provide a quality learning environment in which both students and staff thrive, and to meet the College's Vision and Mission. Personal information held by the College may be disclosed to organisations that assist in the College's fundraising and community relations, for example, the College's fundraising or Old Scholars organisations.

Parents, staff, contractors, volunteers and other members of the wider College community may from time to time receive fundraising information. College publications, like newsletters, annual reports, online posts and year books, which include personal information, may be used for marketing purposes.

Who might the college disclose information to?

The College may disclose personal information, including sensitive information held about an individual to:

- College staff
- Educational institutions
- Government departments;
- Medical practitioners;
- People and/or organisations providing services to the College, including specialist visiting teachers, counsellors and sports coaches;
- Recipients of College publications, such as newsletters, annual reports, online posts and year books;
- Parents;
- Anyone the individual authorises the College to disclose information to; and
- Anyone to whom we are required to disclose information to by law.
- IT system professionals contracted by the College;
- The College's learner management system.

Sending information overseas

The College may disclose personal information about an individual to overseas recipients, for instance, when storing personal information with 'Cloud' service providers which could be situated outside Australia. College exchange or mission or cultural trip would also be a condition when we pass on personal information overseas. However, the College will not send personal information about an individual outside Australia without:

- Obtaining the consent of the individual (in some cases this consent will be implied); or
- Otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

How does the college treat sensitive information?

In referring to 'sensitive information', the College means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless agree otherwise, or the use of disclosure of the sensitive information is allowed by law.

Management and security of personal information

The College's staff are required to respect the confidentiality of students' and parents' personal information and the privacy of individuals.

The College will take all reasonable steps to ensure that information held by the College is accurate and kept up to date.

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

Access and correction of personal information

Under the Privacy Act, an individual has the right to obtain access to a personal information which the College holds about them and to advise the College of any perceived inaccuracy. 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 exceptions to these rights set out in the applicable legislation.

To make a request to access or update any personal information the College holds about a parent or student, contact should be made with the Privacy Officer in writing. The College may require verification of identity and specifications of information required. The College may charge a fee to cover the cost of verifying application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the College will advise the likely cost in advance. If the College cannot provide access to that information, we will provide written notice explaining the reasons for the refusal.

Consent and right access to the personal information of students

The College respects every parent's right to make decisions regarding 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. The College will treat the consent given by parents as consent given on behalf of the student, and notice to parents will act as notice given to the student.

As mentioned above, parents may seek access to personal information held by the College about them or their child by contacting the Principal. However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the College's duty of care to the student.

The College may, at its discretion, on the request of a student grant that student access to information held by the College about them, or allow a pupil 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 so warranted.

Suspected data breaches

The Privacy Act makes it compulsory that organisations report specific types of data breaches (Notifiable Data Breaches) to the affected individuals and also the Office of the Australian Information Commissioner (OAIC).

A data breach occurs where personal information held by the School is lost, exposed or subjected to unauthorised access, modification, unintentional disclosure, or other misuse or interference, or

where these are likely to occur. A Notifiable Data Breach is one that a reasonable person would conclude is likely to result in serious harm – physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

The Act provides for exceptions to a data breach being an eligible data breach, where:

- as a result of remedial action taken by the School in relation to the breach, before it results in serious harm to any individual to whom the information relates, a reasonable person would conclude that the loss, access or disclosure of the information is unlikely to result in serious harm to any of those individuals; or
- if such action were taken in respect of particular individuals prior to serious harm occurring and a reasonable person would conclude that, as a result the loss, access or disclosure would not be likely to result in serious harm to those particular individuals, the School will not be required to notify those individuals of the loss, unauthorised access or unauthorised disclosure.

Examples of data breaches or potential data breaches are:

- A person's personal information is given to another person without the first person's consent e.g. a phone call is received requesting the private mobile phone number of an employee
- Information about a student's learning difficulties being shared or published to a wide group of people
- A school system being 'hacked', and information has been accessed or could have been accessed
- A name and a photo of a student being published (e.g. on the School Facebook page, web site, newsletter or Year Book) after the parent has specifically requested 'do not publish'
- Teacher and student files on the network being accessible by other students due to security permissions being incorrect
- An employee or volunteer accessing personal information on another employee, a volunteer or a student when they have no responsibility to do so i.e. they were accessing the information for private purposes or because they were 'inquisitive'
- An employee using student information to (unsolicited) contact them to invite them to a church youth group activity that they lead
- A device containing sensitive information being lost or stolen
- An email containing personal or sensitive information being mistakenly sent to the wrong person (they have the same last name)
- Information (e.g. financial) of one parent being sent to the estranged/divorced other parent when the School had been told of the separation/divorce
- A staff member disclosing the medical/disability circumstances of one student to another while in casual conversation
- A parent, staff member or student accidentally giving access to the computer files of another person

Data breach procedure

The School will demonstrate that it has taken all appropriate steps to investigate, mitigate, prevent and communicate regarding the breach. This will reduce the likelihood of regulatory intervention and scrutiny. Where a data breach is suspected or believed to have occurred, the School will:

1. Convene a data breach response team, if required. Alternatively, a senior officer shall be made responsible for coordinating the data breach risk assessment and investigation.
2. Carry out a risk assessment (initiate, investigate, evaluate) into the actions or suspicions within 30 days after becoming aware of the breach i.e. action a data breach response plan.
3. Prepare a statement in the prescribed format
4. Submit the statement to the OAIC
5. Contact all affected individuals directly, or if direct contact is not possible or feasible, contact indirectly by publishing information about the data breach on publicly accessible forums.
6. Prepare a comprehensive record and report of the circumstances and the actions taken.

Exceptions to OAIC statement and notification

The following are exceptions to notifying the OAIC of a data breach:

- If Another entity is involved, and that entity having the most direct relationship with the affected individuals has already notified the OAIC
- If notification is likely to prejudice an enforcement activity (e.g. police investigation), and direction not to notify in this regard has been received from the relevant enforcement authority
- If it would be inconsistent with secrecy provisions in other legislation
- If the OAIC has directed that notification will not be required

Data breach response plan

The School has a Data Breach Response Plan to enable the School to contain, assess and respond to data breaches and to help mitigate potential harm to affected individuals. The response plan will include, where appropriate or as directed by the Head of Schools (or delegate) or as directed by the OAIC:

- Engagement of specialist ICT, public relations, legal and other support
- Notification of and engagement with the School's insurer(s)
- Formation of a data breach response team or manager
- Actions which have been directed by the OAIC

Information sharing guidelines

There are circumstances where the School's duty of care for an individual will override privacy concerns. The SA Government recognises that employees in schools are sometime required to share information. These situations are not data breaches.

In these cases, employees of the School are able to share the personal information of a person, usually with authorities or those with responsibility for the care of a person (e.g. a parent), but strictly following the School's policy.

Enquiries and complaints

If further information is required about the way the College manages the personal information it holds please contact the College Principal.

Legislative Context

Children and Young People (Safety) Act 2017
Child Safety (Prohibited Persons) Act 2016
Statutes Amendment (Child Sexual Abuse) Act 2021
Criminal Law Consolidation Act 1935 (SA)
Equal Opportunity Act 1984 (SA)
Sex Discrimination Act 1984 (Cth)
Teacher Registration and Standards Act 2004 (SA)
Education and Early Childhood Services (Registration and Standards) Act 2011(SA)
Education Act 2013 (Cth)
Education Services for Overseas Students Act 2000 (including National Code of Practice for Providers of Education and Training to Overseas Students 2018)
Disability Discrimination Act 1992 (Cth)
Privacy Act 1988 (Cwlth)
Australian Privacy Principles
Privacy Compliance Manual, September 2013, Independent Colleges Council of Australia and National Catholic Education Commission
Standard Collection Notice

Relevant Conventions

National Principles for Child Safe Organisations
The United Nations Conventions of the Rights of the Child

Relevant Standards and Frameworks

Australian Student Wellbeing Framework
National Quality Framework
Protecting Children is Everyone's Business: national framework for protecting Australia's children 2009 – 2020
Child Safe Organisations National Principles
Disability Standards for Education 2005

Relevant Cross Sector Guidelines

Protective Practices for staff in their interactions with children and young people
Managing allegations of sexual misconduct in SA education and care settings
Sexual behaviour in children and young people - Guidelines
Suicide Postvention Guidelines

Relevant Related School Policies and Procedures

Child Protection Policy
Code of Conduct (Staff)
Code of Conduct (Students)
Harassment and Bullying Policy
Volunteer Information Booklet
Grievance & Concerns Policy
Critical Incident/ Emergency Management Policy
Pastoral Care Program

Positive Behaviour Policy
Camps and Excursion Policy
Sexual Harassment Policy
Duty of Care
Medication Policy
Risk Management Policy
Drug Policy
Acceptable Use of Information & Communication Technology (Student) Policy
Acceptable Use of Information & Communication Technology (Staff) Policy

PRIVACY Policy							
Reviewed:	2024	**Next Review Date:**	2027	**Approved by the Principal:**	2024	**Managed by:**	Business Manager