TYNDALE CHRISTIAN SCHOOL
God's Truth Prevails

POLICY NO. A4.02

PRIVACY POLICY

SCOPE OF APPLICATION

This policy is applicable to the following entities, and all departments, businesses and activities operated under the auspices of these entities:

- Tyndale Christian School – Salisbury East
- Tyndale Christian School – Strathalbyn
- Tyndale Christian School – Murray Bridge
- Emmanuel Christian Schools and Ministries

INTERPRETATION

Within this policy, unless specifically defined otherwise, the following terms shall have these meanings:

School or ***schools*** – shall mean all or any one of the Tyndale group of schools

INTRODUCTION

This Privacy Policy sets out how the School manages personal information provided to or collected by it.

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

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.

POLICY

What kinds of personal information does the school collect and how does it collect it?

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

- Students and parents and/or guardians and caregivers ('parents') before, during and after the course of a student's enrolment at the School;
- Job applicants, staff members, volunteers, contractors and specialist service providers; and
- Other people who come into contact with the School.

Personal information you provide

The School 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 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 or reference from another school.

Exception in relation to employee records

Under the Privacy Act, the Australian Privacy Principles do not apply to an employee record. As a result, 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 the employee.

How will the School use the personal information you provide?

The School will use personal information it collects from you 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 reasonably expected by you, or to which you have consented.

Students and parents

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

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

- To keep 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
- To satisfy the School's legal obligations and allow the School to discharge its duty of care.

In some cases where the School requests personal information about a student or parent, if information requested is not provided, 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.

Job applicants and contractors/suppliers

In relation to personal information of job applicants and contractors/suppliers, the School'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 School uses personal information of job applicants and contractors/suppliers include:

- In administering the individual's engagement, as the case may be;
- For insurance purposes;
- Seeking donations and marketing for the School; and
- To satisfy the School's legal obligations, for example, in relation to child protection legislation.

Volunteers

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

Marketing, community relations and fundraising

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

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

Who might the School disclose information to?

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

- Another school;
- Government departments;
- Medical practitioners;
- People providing services to the School, including specialist visiting teachers, counsellors and sports coaches;
- Recipients of School publications, such as newsletters, annual reports and year books;
- Parents;
- Anyone the individual authorises the School to disclose information to; and
- Anyone to whom the School is required by law to disclose information to.

Sending information overseas

The School may disclose personal information about an individual to overseas recipients, for instance, when storing personal information with 'cloud' service providers which are situated outside Australia or to facilitate a school exchange or mission or cultural trip. However, the School 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 School treat sensitive information?

In referring to 'sensitive information', the School 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
- 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 you agree otherwise, or the use of disclosure of the sensitive information is allowed by law.

Management and security of personal information

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

The School has in place steps to protect the personal information the School 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.

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).

Eligible data breaches

An *eligible data breach* occurs where personal information held by the School is lost, exposed or subjected to unauthorised access, modification, disclosure, or other misuse or interference, or where these are likely to occur, and where 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 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.

If a data breach does not meet one of the above exceptions, it is notifiable to the individuals impacted by the breach and to the OAIC.

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 are shared or published to a wide group of people
- A school system is 'hacked', and information has been accessed or could have been accessed
- A name and a photo of a student has been 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 are accessible by other students due to security permissions being incorrect

- An employee or volunteer accesses 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 uses student information to (unsolicited) contact them to invite them to a church youth group activity that they lead
- A device containing sensitive information is lost or stolen
- An email containing personal or sensitive information is mistakenly sent to the wrong person (they have the same last name)
- Information (e.g. financial) of one parent is sent to the estranged/divorced other parent when the School had been told of the separation/divorce
- A staff member discloses the medical/disability circumstances of one student to another while in casual conversation
- A parent, staff member or student is accidentally given access to the computer files of another person

Suspected data breach or risk of data breach

If an employee becomes aware of a suspected data breach which is yet to be proven, or of a risk (possibility) of data breach, that shall be reported to the employee's Executive line manager to initiate the data breach response plan.

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. Ask any employee who suspects a data breach has or may have occurred to notify their Executive Line Manager immediately.
2. The Executive Line Manager is to immediately notify the Head of Schools, the relevant Principal and the Director of Corporate Services of the suspicions. The Head of Schools (or delegate) shall notify the Board of Governors.
3. The Head of Schools (or delegate) shall urgently convene a Data Breach Response Team, with membership appropriate to the size of the data breach. At a minimum, and for very small or straightforward data breaches, a senior officer shall be made responsible for coordinating the data breach response plan (A4.02Z).
4. The Data Breach Response Team shall carry out a risk assessment (initiate, investigate, evaluate) into the actions or suspicions within 30 days after becoming aware of the breach i.e. carry out a data breach response plan (see *A4.02Z Data breach response plan*). The risk assessment will be documented on the *A4.02Y Data breach investigation record*.
5. The Data Breach Response Team shall make recommendations and ensure these are implemented to prevent the data breach or similar data breach from re-occurring.
6. If after the above steps, the eligible data breach is still notifiable, the responsible person will prepare a statement in the prescribed OAIC format.
7. The required statement shall be submitted to the OAIC
8. The Data Breach Response Team shall develop a communications strategy, and this shall include contact with 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.
9. The Data Breach Response Team shall prepare a comprehensive record and report of the circumstances and the actions taken (see *A4.02Y Data breach investigation record*)

Exceptions to OAIC statement and notification

There are exceptions to notifying the OAIC of a data breach:

- Another entity is involved, and that entity having the most direct relationship with the affected individuals has already notified the OAIC
- 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
- It would be inconsistent with secrecy provisions in other legislation
- The OAIC has directed that notification will not be required

Data breach response plan

The School has a Data Breach Response Plan (see *A4.02Z 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 sometimes 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 *S1.16 Information sharing*.

Access and correction of personal information

Under the Privacy Act, an individual has the right to obtain access to a personal information which the School holds about them and to advise the School 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 School holds about a parent or student, contact should be made with the Privacy Officer in writing. The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance. If the School cannot provide you with access to that information, we will provide you with written notice explaining the reasons for the refusal.

Access and correction of personal information is dealt with in more detail in policy A4.03 *Access to personal information*.

Consents and right of access to the personal information of students

The School respects every parent's right to make decisions regarding 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 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 School about them or their child by contacting the Privacy Officer. 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 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 so warranted.

Enquiries and complaints

If individuals would like further information about the way the School manages the personal information it holds, or wish to make a complaint that they believe that the School has breached the Australian Privacy Principles, the individual should contact the School's Privacy Officer. The School will investigate any complaint and will notify the person making the complaint of the decision in relation to the complaint as soon as is practicable after it has been made.

The School has a complaints handling policy A4.04 *Complaints*.

REFERENCES

- Privacy Act 1988 (Cwlth)
- Australian Privacy Principles
- Privacy Compliance Manual, September 2013, Independent Schools Council of Australia and National Catholic Education Commission
- A4.02A Standard collection notice
- A4.02B Old scholars collection notice
- A4.02C Employee collection notice
- A4.02D Contractor supplier collection notice
- A4.02E Volunteer collection notice
- A4.02F Music teacher collection notice
- A4.02G Mission trip participant collection notice
- A4.02H Sports activities collection notice
- A4.02I Instrumental Music Programme collection notice
- A4.02Y Data breach investigation record
- A4.02Z Data breach response plan
- A4.03 Access to personal information
- A4.03A Request for information
- A4.04 Complaints
- L1.20 ELC Privacy and confidentiality
- S1.16 Information sharing policy

TYNDALE
CHRISTIAN SCHOOL
God's Truth Prevails

POLICY INFORMATION

Policy title	A4.02 Privacy policy
Classification	A - Management framework
Sub-classification	A4 - Management policies
Approver	Board of Governors
Date approved	14/08/2018
Date issued	14/08/2018
Officer responsible for this policy	Director of Corporate Services