



<b>Type:</b> Council Policy	<b>Name:</b> Privacy	<b>Policy No:</b> COU POL – 018
<b>Implementation Date:</b> 2010	<b>Last Reviewed:</b> 2018	<b>Review Date:</b> 2020

## Privacy Policy

St Hilda's School (the **School**), as part of the Anglican Church Southern Queensland, is committed to protecting the privacy of its employees, students and parents.

The School is bound by the Australian Privacy Principles (**APPs**) and the *Privacy Act 1988* (Cth) (**the Act**).

### 1. SCOPE

This policy applies to Students, Parents, School Council members, Employees and volunteers. This policy outlines how the School collects, uses and discloses Personal Information.

### 2. DEFINITIONS

**Employee** means all employees employed by the School, including applicants and prospective Employees.

**Employee Record** means a record as defined in the Act.

**Health Information** is a subset of Sensitive Information. It is information or an opinion about the health or disability of an individual and information collected to provide, or in providing a Health Service.

**Health Service** includes an activity performed to assess, record, maintain or improve an individual's health, to diagnose an illness or disability, to treat an individual, or the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

**Notice** means a notice or order issued by The Corporation of the Synod of the Diocese of Brisbane, or any other statutory body to comply with the requirements of section 6K (or as amended from time to time) of the *Royal Commission Act 1902* (Cth).

**Parent** is the parent / guardian / carer of a Student.

**Personal Information** is information or an opinion, whether true or not, and whether recorded in material form or not, about an identified individual or an individual whose identity is reasonably apparent, or can be determined, from the relevant information or opinion.

**Privacy Officer** means Head of Business, Mr Paul Salter, PO Box 290, Southport, QLD, 4215.

**Sensitive Information** is a type of Personal Information. It includes information or opinion 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 preference or practice, or criminal record. Sensitive information also includes biometric information that is used for the purpose of automated biometric verification, biometric identification or biometric templates.

**Student** means prospective, current or past student of the School.

### 3. PURPOSE

The School collects, holds, uses and discloses Personal Information so that it can exercise its function and activities and fulfil relevant duties and obligations.

That may include (but is not limited to):

- (a) informing Parents about the Student's education;
- (b) School administrative purposes, including for the provision of such services to the School;
- (c) supporting a Student's educational, social and medical wellbeing;
- (d) seeking donations and/or marketing for the School; and
- (e) satisfying the legal obligations of the School.

The School collects and holds Personal Information, Sensitive Information and Health Information about Students, Parents and Employees.

The School generally deals with personal and Sensitive Information regarding:

- (f) Students and Parents relating to the enrolment of the Student at the School;
- (g) Employees, volunteers and contractors; and
- (h) other persons who are involved with the School.

The School collects Personal Information about individuals to satisfy legal obligations and to fulfil its educational purpose. If the School requests information to be provided and the request is not complied with, the School may be unable to enrol a prospective Student or continue enrolment of a current Student.

### 4. COLLECTION

#### 4.1 Personal Information

The School collects Personal Information about an individual by way of forms, face-to-face meetings, interviews and telephone calls. Other individuals may provide Personal Information about a person in dealings with the School.

The School may collect Personal Information about an individual from a third party, for example, a medical practitioner providing a report.

Collection of Personal Information from a third party will be undertaken where it is reasonably necessary to do so. Any Personal Information that is unsolicited will be dealt with in accordance with the APPs.

#### 4.2 Kinds of information that the School collects and holds

The type of information that the School collects and holds will depend on the person's relationship with the School. For example:

- **Student:** if the person is a Student of the School, the School may collect and hold information including the Student's name, address, email address, contact telephone number, gender, age, medical history, emergency contact information, Parent information and education results.

- **Employee candidate:** if the person is a candidate seeking employment with the School, the School may collect and hold information about the candidate including the candidate's name, address, email address, contact telephone number, gender, age, employment history, references, resume, medical history, emergency contact information, taxation details, qualifications and payment details.
- **Supplier:** if the person is a supplier to the School, the School may collect and hold information including the supplier's name, address, email address, contact telephone number, business records, billing information, information about goods and services supplied by the supplier.
- **Referee:** if the person is a referee of a candidate being considered for employment by the School, the School may collect and hold information including the referee's name, contact details, current employment information and professional opinion of candidate.

### 4.3 Sensitive Information

Sensitive Information will be collected by the School where it is reasonably necessary for one or more of the School's functions or activities. It will only be collected with consent, unless one of the exceptions under the APPs applies.

### 4.4 Employee Records

Under the Act, the APPs do not apply to employee records. This means that the Act does not apply to how the School deals with an employee record that concerns current and former employees of the School.

Examples of employee records are records of Personal Information regarding:

- The engagement, training, disciplining or resignation of the employee;
- The termination of the employment of the employee;
- The terms and conditions of employment of the employee;
- The employee's personal and emergency contact details;
- The employee's performance or conduct;
- The employee's hours of employment;
- The employee's salary or wages;
- The employee's membership of a professional or trade association;
- The employee's trade union membership;
- The employee's annual, long service, personal, parental or other leave;
- The employee's taxation, banking or superannuation affairs; or
- The employee's Health Information.

The exemption applies to current or former employees. It does not apply to contractors, volunteers or prospective employees.

Despite this exemption, the School may have other obligations regarding employee records, for example under the *Fair Work Act 2009* (Cth) and the *Fair Work Regulations 2009* (Cth).

## **5. USE AND DISCLOSURE**

The School will only use and disclose Personal Information for the primary purpose of collection or as otherwise specified in this Privacy Policy.

The School may disclose Personal Information to the Corporation of Synod of the Diocese of Brisbane for administrative and management purposes including insurance, child protection and professional standards.

Personal information will only be used for a secondary purpose if consent has been obtained, where it is reasonably expected or if such use or disclosure falls within a permitted exception.

Sensitive Information will be used and disclosed for the primary purpose of collection, unless the School is advised otherwise, or the use or disclosure is required / permitted by law.

## **6. QUALITY OF INFORMATION AND SECURITY**

The School endeavours to ensure that the Personal Information it holds is accurate, complete and up to date.

The School will take all reasonable steps to:

- (a) protect Personal Information from misuse, interference, loss, unauthorised access, modification or unauthorised disclosure; and
- (b) destroy or de-identify information that is no longer needed, or not subject to a Notice.

## **7. ACCESS TO PERSONAL INFORMATION**

Access to records of Personal Information that the School holds or concerns about the accuracy of information held by the School should be directed to the Privacy Officer at the School.

Under the Act, an individual has the right to obtain access to Personal Information which the School holds about them; there are exceptions to this, for example, where access may impact the privacy of others or poses as a threat to the individual.

To make a request to access Personal Information the School requires a request in writing. The School will respond to this request within 28 days. Where it is reasonable, the School will provide access in the manner requested. The School may charge a fee to provide access to the Personal Information, however, it will not charge for the request for access.

If a request for access is refused in accordance with the APPs, the School will provide written reasons why the request was refused; details on how to make a complaint will also be included in this response.

The basis upon which access to records can be refused are as follows:

- In the case of Personal Information other than Health Information, that providing access would pose a serious and imminent threat to the life or health of any individual;
- In the case of Health Information, that providing access would pose a serious threat to the life or health of any individual;
- Providing access would have an unreasonable impact upon the privacy of other individuals;
- The request for access is frivolous or vexatious;

- The information relates to existing or anticipated legal proceedings between the School and the individual, and the information would not be accessible through the process of discovery in those proceedings;
- Providing access would reveal the School's intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- Providing access would be unlawful;
- Denying access is required or authorised by or under law (such as in relation to legally privileged information);
- Providing access would be likely to prejudice an investigation of possible unlawful activity;
- Providing access would be likely to prejudice:
  - The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
  - The enforcement of laws relating to the confiscation of the proceeds of crime;
  - The protection of the public revenue;
  - The prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
  - The preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders.

## **8. UPDATING THE ACCURACY OF RECORDS**

If the School holds Personal Information that is inaccurate, out-of-date, incomplete, irrelevant or misleading, it will take steps as are reasonable to correct the information.

If the School holds Personal Information and a person makes a request in writing addressed to the Privacy Officer to correct the information, the School must take steps as are reasonable to correct the information, and the School will respond to any request within a reasonable period.

There are certain circumstances in which the School may refuse to correct the Personal Information. In such situations the School will give the person written notice that sets out:

- (a) the reasons for the refusal; and
- (b) the mechanisms available to the person to make a complaint.

If the School corrects Personal Information that it has previously supplied to a third party and a person requests us to notify the third party of the correction, the School will take such steps as are reasonable to give that notification unless impracticable or unlawful to do so.

## **9. STORING AND ARCHIVING RECORDS**

Personal information is stored in hard copy and electronically.

## **9.1 Hard copy records**

Hard copy files are to be stored in locked storage, be it onsite or offsite. Access to these records is restricted to authorised School employees.

All authorised School employees must ensure that all papers and files relating to School Employees are stored in locked areas at night, when authorised employees are absent from the office or at other times when authorised employees are not working on such papers or files.

Any destruction of copies of documents or unwanted pieces should be by way of secure destruction bin or shredding.

## **9.2 Electronic files**

All electronic correspondence or other electronic documents regarding Personal Information are filed in the appropriate employee file in the School's document storage solution. Only authorised employees have access to these files. Authorised employees may only access electronic or hard copy files for the purposes set out under Section 5 and no other purpose.

Any person who accesses a file for an unauthorised purpose will be subject to disciplinary action, including where appropriate, dismissal.

# **10. DE-IDENTIFICATION AND DESTRUCTION OF RECORDS**

## **10.1 Hardcopy Tax File Number (TFN) Declarations**

Where the School receives completed hard copy TFN Declaration Forms, the Tax File Number must be "blacked" out once the details have been entered into the payroll system. The Form should then be placed in the employee's personnel file.

## **10.2 Electronic Tax File Number (TFN) Declarations**

Where Employees submit their TFN Declaration electronically, the record is contained electronically in the organisation's document storage solution. Only authorised employees have access to these files.

## **10.3 Archiving and Destruction**

Unless subject to a relevant Notice, the School is required to keep time and wages records for its employees for seven years.

After 7 years, the School will destroy any physically stored employment records in a secure way and for Personal Information contained in an electronic form the School will ensure that this information is put in a form beyond use.

In circumstances where the School is subject to a Notice in relation to the retention of documents, the School must comply with the terms of that Notice.

# **11. OVERSEAS DISCLOSURE AND CLOUD**

The School may disclose Personal Information about an individual overseas; this is likely to occur if the School uses "cloud" service providers.

When disclosing Personal Information the School will take all steps reasonable to ensure that the overseas recipient complies with the APPs.

The countries in which overseas recipients are likely to be located include, but are not limited to United States of America.

## **12. MARKETING AND FUNDRAISING**

The School engages in marketing and fundraising as a means to promote future growth and sustain and improve the educational environment for Students.

Personal information collected may be used to make a marketing or fundraising appeal. The School will abide by any direction from an individual not to disclose Personal Information to third parties for marketing purposes.

The School also allows individuals to “opt out” through selection on the Standard Collection Notice, or on the enrolment agreement.

## **13. NOTIFIABLE DATA BREACHES**

### **13.1 What is a Notifiable Data Breach?**

A Notifiable Data Breach occurs when Personal Information of an individual held by the School is accessed by, or is disclosed to, an unauthorised person, or is lost, and:

- (a) a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual; or
- (b) in the case of loss (i.e. leaving a laptop containing Personal Information on a bus), unauthorised access or disclosure of Personal Information is likely to occur, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual.

### **13.2 Assessment**

If the School suspects that a Notifiable Data Breach has occurred, it will conduct a reasonable and expeditious assessment to determine if there are reasonable grounds to believe that a Notifiable Data Breach has occurred.

The School will take all reasonable steps to ensure that the assessment is completed within 30 days of becoming aware of the suspected Notifiable Data Breach.

### **13.3 Notification**

Subject to any restriction under the Act, in the event a Notifiable Data Breach occurs, the School will, as soon as practicable, prepare a statement outlining details of the breach, and:

- (a) notify the individual of the unauthorised access, disclosure or breach; and
- (b) notify the Office of the Australian Information Commissioner of the unauthorised access, disclosure or breach.

## **14. COMPLAINTS**

If an individual believes that the School has breached the APPs a complaint can be made to the School.

All complaints should be in writing and directed to the Privacy Officer. The School will investigate complaints in a timely manner and respond in writing.

If an individual is not satisfied with the School's response, a complaint can be lodged with the Office of the Australian Information Commissioner on the following website  
<http://www.oaic.gov.au/privacy/making-a-privacy-complaint>.

#### **15. CONTACT DETAILS**

MR PAUL SALTER

HEAD OF BUSINESS

ST HILDA'S SCHOOL

PO BOX 290,

SOUTHPORT, QLD 4215

(07) 55 324 922

#### **16. PUBLICATION AND REVIEW DATE DETAILS**

INITIAL PUBLICATION: FEBRUARY 28, 2018

REVISED: MAY 29, 2018



ST HILDA'S SCHOOL  
GOLD COAST

## STANDARD COLLECTION NOTICE

ST HILDA'S SCHOOL  
52 HIGH ST, SOUTHPORT, QLD, 4215

1. St Hilda's School (**the School**) collects Personal Information, including Sensitive Information about students and parents before and during the course of the student's enrolment at St Hilda's School.
2. The primary purpose of collecting information is to allow the School to exercise its functions and activities and ultimately provide schooling to your daughter.
3. The School collects, uses, holds and discloses Personal Information in accordance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (**APPs**).
4. Legislation that governs public health and child safety requires that certain types of information be collected by the School.
5. The information that the School collects is to satisfy legal obligations and enables the School to discharge its duty of care.
6. The School collects Health Information about students. Health information is a subset of Sensitive Information; it is defined in the *Privacy Act 1988* (Cth) and is dealt with in accordance with the APPs.
7. If the School does not obtain the information referred to above, it may not be able to enrol or continue the enrolment of your daughter.
8. Personal and Sensitive Information collected by the School may be disclosed to others for administrative and educational purposes. This would include disclosure to other schools, government departments, the Corporation of the Synod of the Diocese of Brisbane, the Anglican Church Southern Queensland and other persons providing services to the School.
9. Personal information collected from students is generally disclosed to parents. Personal information and images (for example, sporting and academic achievements) is published in the school newsletter, magazine and may be used for other School related purposes. Please inform the School in writing if information in relation to your daughter's is not to be used in this manner.
10. Personal information collected may be disclosed by the School to debt collection agencies for the purpose of recovering outstanding tuition fees.
11. Parents may seek to access information collected about their daughter by contacting the School. Access to Personal Information is dealt with in accordance with the School's Privacy Policy.
12. Parents may seek to have Personal Information corrected. Correction of Personal Information is dealt with in accordance with the School's Privacy Policy.
13. Parents or students may make a complaint in accordance with the School's Privacy Policy if they believe the School has breached the APPs.

14. The School may store and disclose Personal Information to overseas recipients, through the usage of Cloud Computing Storage or similar services. The School discloses such information in accordance with APP 8 and discloses to United States of America.
15. The School engages in fundraising activities. Personal information collected may be used to make a marketing or fundraising appeal. The School will abide by any direction from an individual not to disclose Personal Information to third parties for marketing purposes.

I **do not** want my Personal Information used for direct marketing

16. A copy of the School's Privacy Policy can be found at [www.sthildas.qld.edu.au](http://www.sthildas.qld.edu.au).

Student's Name:

Year Level:

Year of Entry:

Parent's Signature:

Date: