

1.0 SCOPE	2
2.0 DEFINITIONS	2
2.1 Employee	2
2.2 Employee Record	2
2.3 Health Information	2
2.4 Health Service	2
2.5 Notice	2
2.6 Parent	2
2.7 Personal Information	2
2.8 Privacy Officer	2
2.9 Sensitive Information	2
2.10 Student	2
3.0 PURPOSE	3
4.0 COLLECTION	3
4.1 Personal Information	3
4.2 Kinds of information that the College collects and holds	3
4.3 Sensitive Information	4
4.4 Employee Records	4
5.0 USE AND DISCLOSURE	4
6.0 QUALITY OF INFORMATION AND SECURITY	4
7.0 ACCESS TO PERSONAL INFORMATION	4
8.0 UPDATING THE ACCURACY OF RECORDS	5
9.0 STORING AND ARCHIVING RECORDS	5
9.1 Hard copy records	6
9.2 Electronic files	6
10.0 DE-IDENTIFICATION AND DESTRUCTION OF RECORDS	6
13.1 Hardcopy Tax File Number (TFN) Declarations	6
13.2 Electronic Tax File Number (TFN) Declarations	6
13.3 Archiving and Destruction	6
11.0 OVERSEAS DISCLOSURE AND CLOUD	6
12.0 MARKETING AND FUNDRAISING	6
13.0 NOTIFIABLE DATA BREACHES	7
13.1 What is a Notifiable Data Breach?	7
13.2 Assessment	7
13.3 Notification	7
14.0 COMPLAINTS AND CONTACT DETAILS	7
15.0 PUBLICATION AND REVIEW DATE DETAILS	7

1.0 SCOPE

West Moreton Anglican College (the **College**), as part of the Anglican Church Southern Queensland, is committed to protecting the privacy of its employees, students and parents. The College is bound by the Australian Privacy Principles (**APPs**) and the Privacy Act 1988 (Cth) (**the Act**). This policy applies to Students, Parents, College Council members, Employees and volunteers. This policy outlines how the College collects, uses and discloses Personal Information.

2.0 DEFINITIONS

2.1 **Employee**

Means all employees employed by the College, including applicants and prospective Employees.

2.2 **Employee Record**

Means a record as defined in the Act

2.3 **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.

2.4 **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.

2.5 **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).

2.6 **Parent**

Is the parent / guardian / carer of a Student.

2.7 **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.

2.8 **Privacy Officer**

Means insert person, and contact details (Head of Risk).

2.9 **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.

2.10 **Student**

Means prospective, current or past student of the College.

3.0 PURPOSE

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

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

The College generally deals with personal and Sensitive Information regarding:

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

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

4.0 COLLECTION

4.1 *Personal Information*

The College 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 College.

The College 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 College collects and holds*

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

- **Student:** if the person is a Student of the College, the College 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 College, the College 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 College, the College 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 College, the College 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 College where it is reasonably necessary for one or more of the College'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 College deals with an employee record that concerns current and former employees of the College.

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 College may have other obligations regarding employee records, for example under the Fair Work Act 2009 (Cth) and the Fair Work Regulations 2009 (Cth).

5.0 USE AND DISCLOSURE

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

The College 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 College is advised otherwise, or the use or disclosure is required / permitted by law.

6.0 QUALITY OF INFORMATION AND SECURITY

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

The College 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.

7.0 ACCESS TO PERSONAL INFORMATION

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

Under the Act, an individual has the right to obtain access to Personal Information which the College 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 College requires a request in writing. The College will respond to this request within a reasonable period of time 14 days, but no more than 30 days. Where it is reasonable, the College will provide access in the manner requested. The College 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 College 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 College and the individual, and the information would not be accessible through the process of discovery in those proceedings;
- Providing access would reveal the College'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.

8.0 UPDATING THE ACCURACY OF RECORDS

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

There are certain circumstances in which the College may refuse to correct the Personal Information. In such situations the College 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 College 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 College will take such steps as are reasonable to give that notification unless impracticable or unlawful to do so.

9.0 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 College employees.

All authorised College employees must ensure that all papers and files relating to College 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 College'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.

10.0 DE-IDENTIFICATION AND DESTRUCTION OF RECORDS

13.1 Hardcopy Tax File Number (TFN) Declarations

Where the College 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.

13.2 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.

13.3 Archiving and Destruction

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

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

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

11.0 OVERSEAS DISCLOSURE AND CLOUD

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

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

12.0 MARKETING AND FUNDRAISING

The College 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 College will abide by any direction from an individual not to disclose Personal Information to third parties for marketing purposes.

The College also allows individuals to "opt out" through selection on the Standard Collection Notice, or on the enrolment agreement.

13.0 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 College 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 College 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 College 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 College 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.

14.0 COMPLAINTS AND CONTACT DETAILS

If an individual believes the College has breached the APPs a complaint can be made in writing to the Principal.

Complaints will be investigated in a timely manner and a written response provided within a reasonable timeframe of up to 30 days.

The Principal may delegate these responsibilities.

CONTACT DETAILS: The Principal, West Moreton Anglican College
Locked Bag 8004, Ipswich Queensland 4305
T: 07 3813 4555 F: 07 3813 4566

If an individual is not satisfied with the College'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>.

15.0 PUBLICATION AND REVIEW DATE DETAILS

Policy effective as at 10 December 2018 with a review date set annually.