Privacy Policy

1. Purpose

The Corporation of the Synod of the Diocese of Brisbane trading as Toowoomba Anglican School ABN 44 882 391 796 as part of the Anglican Church Southern Queensland, (the "School", "we", "us", "our"), is committed to protecting and managing the privacy and personal information of employees, students and parents in accordance with Australian Privacy Principles (APPs) and the Privacy Act 1988 (Cth) (the Act).

This document is referred to as our Privacy Policy and sets out our policies for managing personal information including how we collect, use, hold, store and disclose personal information.

2. Scope

This Privacy Policy applies to students, parents, council members, employees, volunteers and other community members who are referred to in this Privacy Policy as "you", "your" or "individual".

3. Policy Statement

This Privacy Policy applies to your personal information regardless of how we collect it from you. When you submit information to us, access or use our websites, mobile application or social media platforms, you are providing your consent to us collecting and managing your personal information according to this Privacy Policy.

This policy is effective as of 5 March 2025. From time to time, we may need to change this Privacy Policy, and will post the updated version on our website at https://www.taschool.qld.edu.au/terms-and-privacy/ Any such amendments will take effect immediately after such posting. Please check this Privacy Policy regularly for any updates.

4. Definitions

Term	Definition
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 defined under the Act and includes: (a) information or an opinion about: (i) the health, including an illness, disability or injury, (at any time) of an individual; or (ii) an individual's expressed wishes about the future provision of health services to the individual; or

	(iii) a health service provided, or to be provided, to an individual; that is also personal information; (b) other personal information collected to provide, or in providing, a health service to an individual; (c) other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances; (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.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.
Parent	is the parent / guardian / carer of a Student.
Personal Information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in material form or not.
Privacy Officer	means a nominated Toowoomba Anglican School representative contactable on 07 4639 8111.
Sensitive Information	is defined in clause 4.3. below
Student	means prospective, current or past student of the School.

5. 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):

- informing Parents about the Student's education;
- School administrative, management, operational and financial purposes, including for the provision of such services to the School;
- supporting a Student's educational, social and medical wellbeing;
- marketing or other promotional purposes of the School;
- recruitment of Employees including volunteers, internships and work experience;

- managing, planning, advertising and administering programs, events, competitions and performances for the School;
- to provide interactive features and communication methods for us to communicate with you through our mobile device applications and/or Website;
- to ensure the safety and security of the School;
- seeking donations and for the School; and
- satisfying the legal obligations of the School.

The School collects and holds personal information, sensitive information and health information about individuals including Students, Parents and Employees.

The School collects personal information about individuals to satisfy legal obligations and to fulfil its educational purpose. You can always decline to give us your personal information, but that may mean that the School may be unable to enrol a prospective Student, continue enrolment of a current Student, employ you as an Employee or otherwise provide our educational services to you.

6. Collection

6.1. Personal Information

The School collects personal information, sensitive information and health information about an individual by way of forms, face-to-face meetings, interviews, telephone calls, by email, through our website over the internet including through our social media sites. 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 or a Parent.

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.

6.2. 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 and may include:

- Contact Information & Personal Data: your name, date of birth, age, gender, address, email address, and telephone details.
- Government Related Identifiers: your tax file number, Medicare number, Individual Healthcare identifier and others.
- Payment Details: your credit card, bank account details, and billing information to complete purchases.
- Financial Details: your financial details and occupation, which may include budget information, wages/salary information, and general expenditure.

- Identification Documents: your driver's licence, birth certificate, passport or other photographic identification documents.
- Photographs & Videos: any pictures, videos, sound recordings and other audio-visual recordings that you provide to us, or authorise us to take of you in accordance with our media consent form.
- Videos or images captured using surveillance device: when you enter our premises we may collect images or audio-visual recordings of you through security cameras or CCTV contained in or around our premises.
- Geo-Location & Locality Information: when you interact with us, we may collect your current or last known location used to determine your locality from other individuals. We may achieve this through various methods, including collecting your Wi-fi, Global Positioning System (GPS), Cellular or other technology in your electronic device or web browser.
- Cookies & Other Browser or Device Information: your session cookies and persistent cookies when you visit our website, your device type, browser type, Internet Protocol (IP) address, your URL information, the date and time (including time zone) of your visit, the pages you have accessed on our websites and third party websites, your software and hardware information concerning your mobile device or computer. Cookies that we place may be removed by following instructions that are provided by your browser.
- Interaction & Behavioural Information: your interactions, use, habits, behaviours when dealing with us, our website and other applications.
- Employment Information: We collect personal information when recruiting Employees, such as your name, contact details, qualifications and work history. Generally, we will collect this information directly from you. We may also collect personal information from third parties in ways which you would expect (for example, from recruitment agencies or referees you have nominated). Before offering you a position, we may collect additional details such as your tax file number and superannuation information and other information necessary to conduct background checks to determine your suitability for certain positions (for example, positions which involve working with children).
- Other Information: any other administrative and additional information that you provide to us, or authorise us to collect, as a part of your interaction with the School.

6.3. 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.

When we refer to sensitive information, we are referring to certain personal information that is more sensitive.

Sensitive information means:

1. information or an opinion about an individual's:

   (a) Racial or ethical origin;
   (b) Political opinions;
   (c) Membership of a political association;

(d) Religious beliefs or affiliations;
(e) Philosophical beliefs;
(f) Membership of a professional or trade association;
(g) Membership of a trade union;
(h) Sexual orientation or practices; or
(i) Criminal record,

that is also personal information, or

2. Health information about an individual;
3. Genetic information about an individual that is not otherwise health information;
4. Biometric information that is used for the purpose of automated biometric verification or biometric identification; or
5. Biometric templates.

Under the APPs, sensitive information is afforded a higher level of privacy protection and requires us to obtain your consent before collecting this type of information. We do not regularly collect sensitive information and if we need to collect sensitive information about you, for example, to provide you with our services we will ask for your consent prior to collecting this type of information.

It will only be collected with consent, unless one of the exceptions under the APPs applies.

6.4. 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.

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

If requested by a current or former employee, and with that employee's written consent, the Toowoomba Anglican School may provide written employee references to prospective employers. If the Toowoomba Anglican School decides to provide a reference, the reference may include information on the following:

- The employee's tenure at the school
- The employee's role(s) and responsibilities whilst employed by Toowoomba Anglican School
- A balanced appraisal of the employee's capabilities and performance in carrying out their assigned duties, whilst employed at Toowoomba Anglican School.

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).

6.5. Financial Information

Financial information will be collected by the School where it is reasonably necessary for the operation of a fees account with the School. Such information may include financial details such as credit eligibility information. Credit Eligibility Information means information that has been obtained from a CRB [a Credit Reporting Body], or personal information that has been derived from

that information, that is about an individual's consumer credit worthiness. The kind of information we might derive from an individual's consumer credit report includes:

- A credit assessment relating to the individual;
- An unsuitability assessment relating to the individual;
- And any internal credit scores.

6.6. Students and Minors

We may collect personal information about Students and other individuals below the legal age of majority (Minors) (for example, when children participate in events we are involved with). Where those Minors do not have sufficient maturity and understanding to make decisions about their personal information, we will require their Parents or guardians to make decisions on their behalf. However, we are unable to distinguish the age or identity of the people accessing and using our website or social media platforms or mobile application, or who attend events or activities run by us. This may result in the accidental collection of personal information from Minors without the consent of a parent or guardian. If this does occur, then we recommend that you contact us and ask for the personal information to be de-identified or destroyed.

7. Use and Disclosure

The School will only use and disclose personal information for the primary purpose with which it was collected 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;
- the School's engaged contractors, agents or suppliers who assist us with operating the School;
- payment and debit service providers and processors;
- our market research service providers and digital marketing agents;
- our professional advisors, such as our lawyers, accountants and financial advisors;
- relevant courts, tribunals or regulatory authorities and law enforcement bodies; and
- anyone else to whom you authorise us to disclose your information or that would be reasonably expected.

The School takes reasonable steps to ensure that the third parties we engage, take reasonable steps to protect your personal information following the APPs and in a similar manner with this Privacy Policy. Our third-party service providers are required only to use the personal information disclosed to them by us for the purpose that it was provided to them. Additionally, the third parties to who we have disclosed your personal information may contact you directly to let you know they have collected your personal information and give you information about their privacy policies.

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.

Financial information will be used and disclosed for the primary purpose of which it was collected, as relevant to our business relationship with you.

8. 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:

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

For example, we may maintain computer and network security, use firewalls and other security methods and other security systems such as user identifiers and passwords to control access to our computer systems and data transfer encryption protocols and network monitoring systems to protect data.

Please be aware that there is no method of transmission of information over the internet or through electronic storage that is fully secure and safe. We cannot guarantee the security of your personal information that we hold, but we do take reasonable steps to protect your information. If we are required by law to inform you of any misuse, interference, loss or unauthorised of your personal information, then we will notify you electronically, in writing or by telephone.

Our websites, applications or email systems may not use encryption or other technologies to ensure the secure transmission and receipt of information via the internet. Anyone using our website or receiving an email from us is encouraged to exercise care in sending personal information or depositing money via the internet. We recommend that you refrain from clicking any unsecured links or opening unknown attachments.

If you hold any concerns or become suspicious of any misuse, interference, loss or unauthorised access to our website, our email systems or to our business more generally, we ask that you contact us immediately to verify your concern or suspicion.

9. 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.

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 pose 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 a reasonable period of time. 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, will not charge for the request for access.

If a request for access is refused the School will provide written reasons on 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 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 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 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.

10. 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:

- The reasons for the refusal; and
- 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.

11. Storing and Archiving Records

The School may hold and store your personal information in paper-based files, or electronic record keeping methods in secure databases (including trusted third party storage providers based in Australia and overseas, which may include cloud-based storage providers).

11.1. 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.

11.2 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.

11.3 Third-party storage

Your personal information may be collected in electronic form for use or storage with a third-party storage provider that we engage.

We cannot ensure that your personal information is or will remain secure. This is due to us not having control over the third-party provider's policies and procedures concerning the handling and storing of your personal information.

The School may also use Google Analytics to help us understand how our Students and Parents use our platforms, website or educational services. You can read more about how Google uses your Personal Information via https://www.google.com/intl/en/policies/privacy/. You may also opt-out of Google Analytics here: https://tools.google.com/dlpage/gaoptout.

12. De-Identification and Destruction of Records

12.1 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.

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.

12.2 Remaining Anonymous & De-Identified

The School may require you to provide specific details and information to enable us to provide our services to you. We try to allow you to stay anonymous or use a pseudonym in your dealings with us where it is lawful and practicable to do so. For example, when making a general and nonspecific enquiry. Typically, it is not possible for us to deal with you anonymously or pseudonymously on an ongoing basis. If we do not collect your personal information, you may not be able to utilise our services, attend our School, deal with us or participate in our events, programs or activities we manage or deliver.

12.3 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 seven years, the School will destroy any physically stored time and wages 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 the Notice.

13. 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. Accordingly, there may be mechanisms available to you to enforce the protection of your personal information under that overseas law. In the circumstances, we do not require the overseas recipients to comply with the APPs, and we will not be liable for a breach of the APPs if your personal information is mishandled. We also disclaim responsibility to the extent permitted by law and note that you may not have a remedy under Australian law.

The countries in which overseas recipients are likely to be located include, but are not limited to Asia Pacific Region and the Northern California Availability Zones in the US West Region.

Given the current global economy and the ability for information to be shared across borders, the School is taking the following reasonable steps to try and ensure data security:

- No personal information will be sent as email attachments unless the individual has requested this in writing;
- Personal information and data collected by the School is managed by an Australian based third party provider who implements a range of data security measures and practices including continuous threat detection and network traffic analysis, data protection policies, encryption and secure storage, access control and monitoring and incident response planning.
- If we transfer your personal information outside of Australia, we will comply with requirements of the Act that relate to trans-border data flows. While we will not directly disclose your personal and/or sensitive information to overseas recipients, without your consent, the entities to which we may disclose personal information may do so.

14. European Union General Data Protection Regulation

The European Union (EU) General Data Protection Regulation (GDPR) contains new data protection requirements and is effective as of 25 May 2018. GDPR replaces national privacy and security laws that previously existed within the EU with a single, comprehensive EU-wide law that governs the use, sharing, transferring and processing of any personal data that originates from the EU. The GDPR applies to the data processing activities of businesses, regardless of size, that are data processors or controllers with an establishment in the EU.

Consequently, Australian businesses of any shape and size may need to comply if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU. There are also some notable differences, including certain rights of individuals (such as the 'right to be forgotten') which do not have an equivalent right under the APPs and the Privacy Act.

Currently, the GDPR does not apply to the School as we do not currently offer our services to individuals located in Europe, our website does not explicitly target customers located in the EU nor do we monitor the behaviour of individuals in the EU.

15. 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 our Standard Collection Notice or by contacting our Privacy Officer informing them that you want to opt-out of receiving marketing material from us. If you opt-out of receiving marketing material, we may still contact you concerning any ongoing relationship with you.

16. 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.

We will contact you within thirty (30) days of the date we receive the written details of your complaint to acknowledge that we have received it. We may ask you to provide further information about your complaint and the outcome you are seeking.

Our privacy officer will review the way we dealt with your personal information, conduct an internal investigation (if necessary) into the complaint and will likely respond to you within thirty (30) days of the date we acknowledged receipt of your complaint. We will then typically gather relevant facts, locate and review relevant documents and speak with individuals involved.

In most cases, we will investigate and respond to a complaint within sixty (60) days of receipt of the complaint. If the matter is more complex or our investigation takes longer than anticipated, we will let you know.

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.

17. Contact Details

We welcome any comments or questions about our Privacy Policy. All enquiries should be directed to the School's Privacy Officer at the following contact details:

Privacy Officer
Toowoomba Anglican School 2 Campbell Street
TOOWOOMBA QLD 4350
Phone: 07 4639 8111
Email: privacyofficer@taschool.qld.edu.au

18. Relevant Legislation

- Privacy Act 1988 (Cth)
- Information Privacy Act 2009 (QLD)
- Right to Information Act 2009 (QLD)
- Freedom of Information Act 1992 (QLD)
- Australian Privacy Principles

19. Policy Information

Accountable Officer	Privacy Officer
Responsible Committee	School Council
Policy Framework	Risk Management Framework
Record Number	TAS_PRIPOL_01
Revision Number	2
Approval Date	February 2025
Publish Date	March 2025
Review Date	February 2027