St Clair Anglican Church - Master Privacy Policy

Our Approach to Privacy

We are a parish within the Anglican Church Diocese of Sydney which is bound by the Privacy Act 1988 (the **Privacy Act**) and which has elected to comply with the Sydney Anglican Master Privacy Policy.

The Privacy Act contains 10 National Privacy Principles (the **NPPs**) which specify how organisations should handle personal information.

St Clair Anglican Church has developed its own set of privacy principles which embody the NPPs. This document details our approach to information privacy and the way we collect, use and protect personal information.

This Policy sets out the St Clair Anglican Church Privacy Principles and the procedures we use when handling personal information.

St Clair Anglican Church staff and those acting on behalf of the staff are required to comply with this Policy when handling personal information.

What does this Policy cover?

This Policy sets out:

- the **standard** by which we handle personal information;
- the rights of individuals to **access** the personal information which we hold about them or to make a **complaint** about how we have handled their **information**; and
- who to contact if you would like to know more about our approach to privacy.

This Policy is designed for use by our staff and to inform others, where necessary, of our approach to privacy.

Where do I go to find out more?

If you would like to know more about the Privacy Act and how it impacts on private sector organisations, visit the website of the Federal Privacy Commissioner http:/www.privacy.gov.au/.

If you would like more information about the way we use personal information, contact our Privacy Compliance Officer (the **PCO**). Our PCO's contact details are out the end of this Policy.

1. ## NPP 1 – Collection

Privacy Principle

*We will generally collect only the personal information we **need** to provide and facilitate our ministries and services. Our aim is to use **fair** and **lawful** ways to collect it.*

*We will usually ensure we have **consent** to collect **sensitive** information.*

*Where reasonably practicable we attempt to collect personal information **directly** from individuals. We will usually take reasonable steps, when we collect information, to ensure that you know **why** we are collecting it, **who** we give it to and **how** we will use or disclose it. This is the case whether we collect it from the individual or from someone else.*

What Does This Mean?

Personal information is any information, including an opinion, about a person that can be used to identify the person, for example, a person's name or address.

Particular types of personal information are considered to be **sensitive information** and are subject to a higher degree of protection. Sensitive information is information or opinion about a person's:

- religious or philosophical beliefs and affiliations;
- racial or ethnic origin;
- political opinions or membership of a political association;
- membership of professional or trade associations;
- membership of a trade union;
- sexual preferences or practices;
- criminal record; or
- health.

We will generally only collect the personal information which we need to provide and facilitate our ministries and services.

Where possible, we will:

- collect personal information in a way which is fair and open;
- not make unreasonably intrusive enquiries; and
- try to collect personal information from individuals directly.

When collecting personal information, we will take reasonable steps to let the individual know the purposes for which the information is being collected and to whom, if anyone, the information is likely to be disclosed. Sometimes this will not be necessary, for example, where it is clear from the context why we are collecting the information.

Where relevant, we will tell an individual of any consequences of not providing the information and, if applicable, identify any law requiring the collection of the information. If we ask for information later we will usually explain why we need it. We will also include our contact details so individuals are aware of how to contact us should they wish to access the personal information we hold about them.

We may collate information about individuals which is received from others, including public sources, with the information we have obtained directly from the individual. If we do get information from someone else, we will take reasonable steps to make sure the individual is aware we have collected or may collect information of that type or from that source (unless the individual has already authorised that person to give us the information).

2. NPP 2 - Use and Disclosure

Privacy Principle

*We will usually only **use** or **disclose** personal information for:*

- the **primary purpose** for which it was collected;
- a **related** purpose which the individual would reasonably expect; or
- with consent,

*unless an **exception** applies.*

What Does This Mean?

Where possible, we will use personal information for the main purpose for which it was provided to us.

Generally, we use personal information to provide and facilitate our ministries and services to our members, and members of the local community with whom we have contact. We also use it to enhance and develop our relationship with our members and the local community.

If the purposes for which we have collected the information involve providing personal information about an individual to any third party, we will take appropriate and reasonable steps to ensure any personal information is protected.

As a general rule, we will use or disclose information for a secondary purpose if the person has consented or if it is related to the primary purpose (and, if the information is sensitive information, directly related to the primary purpose), and the individual who is the subject of the information would reasonably expect the information to be used for such a purpose. This may apply, for example, if we share personal information with other entities who are members of the Anglican Church Diocese of Sydney.

Use Without Consent

Situations in which we may use or disclose information without an individual's consent include where:

- we reasonably believe that use or disclosure is necessary to reduce or prevent a threat to a person's life or health or safety or a serious threat to public health or safety;
- we are investigating or reporting on suspected unlawful activity;
- the use or disclosure is required or authorised by law; or
- we reasonably believe that the use is necessary for law enforcement, public revenue protection, prevention and remedying of seriously improper conduct, or preparation or conduct of court or tribunal proceedings, either by or on behalf of an enforcement body.

If we use or disclose information on these grounds we will make a written note of such disclosure.

Sharing Information

We may share personal information with other entities, including entities that are located outside Australia. If we transfer personal information outside Australia we will do so in accordance with NPP 9.

The Privacy Act allows information (other than sensitive information, which must not be shared without consent) to be shared between related companies or organisations provided we have taken reasonable steps to tell the individual that we may do this. This means that the related bodies corporate within the Anglican Church Diocese of Sydney may deal with information as if they were one organisation.

3. NPP 3 - Data Quality

Privacy Principle

*We will take reasonable steps to introduce systems to ensure that personal information we hold is **accurate** and **current**.*

What Does This Mean?

We will take reasonable steps to ensure that the personal information that is collected, used and disclosed by us is accurate, complete and up-to-date. This means that if we become aware of any change in personal information we will update our records.

4. NPP 4 - Data Security

Privacy Principle

*We will implement measures to protect personal information from **misuse**, **loss** and **unauthorised access, changes** or **disclosure**. We will usually **destroy** or **permanently de-identify** personal information when we no longer need it.*

What Does This Mean?

We will take reasonable steps to keep the personal information we hold secure from misuse, loss and unauthorised access.

We will take reasonable steps to destroy or remove identifying features from personal information when it is no longer needed for any purpose including any requirement of law.

5. NPP 5 - Openness

Privacy Principle

*We will be **open** about how we manage personal information. If asked, we will provide more information about our approach to privacy.*

What Does This Mean?

This document exists to explain our approach to privacy. Copies of this document are available to individuals who want to know more about our policies on managing personal information.

If asked, we will take reasonable steps to let individuals know the sort of personal information we hold, the purpose for which hold it and how we collect, use, store and disclose the information.

Contact our PCO for a copy of any of this document or if you would like more information about the way we handle personal information.

6. NPP 6 - Accessing and Correcting Personal Information

Privacy Principle

*Usually, when asked, we will give an individual **access** to their personal information unless there is a reason why we cannot do so.*

What Does This Mean?

Individuals have a right to ask us what sort of personal information we hold about them.

As a general rule, we will allow an individual access to the personal information we hold about them within a reasonable time after access is requested, unless there is a reason why we cannot do so.

Sometimes there will be a reason why we cannot provide access or we decide not to give access to a record following a request.

We may deny a request for access if we reasonably believe any of the following circumstances apply:

- it would pose a serious and imminent threat to the life or health of any person or, if health information, would pose a serious threat to the life or health of any person;
- the privacy of others would be unreasonably affected;
- the request is frivolous or vexatious;
- the information relates to existing legal proceedings with the person who is the subject of the information and would not be accessible through discovery;
- providing access would prejudice negotiations with the person who is the subject of the information by revealing our intentions regarding those negotiations;
- providing access would be unlawful or denying access is required or authorised by law;

- providing access would be likely to prejudice an investigation of possible unlawful activity;
- providing access would be likely to prejudice law enforcement, public revenue protection, prevention and remedying of seriously improper conduct, or preparation or conduct of court or tribunal proceedings, either by or on behalf of an enforcement body;
- an enforcement body performing a lawful security function requests denial of access to protect national security; and
- where evaluative information generated by us in making a commercially sensitive decision would be revealed by providing access. In this situation we may provide an explanation for the commercially sensitive decision instead.

If we refuse access, we will usually explain why.

In responding to a request to provide access, we will consider using a mutually agreed intermediary if it is reasonable to do so in the circumstances.

We will take reasonable steps to correct personal information we hold if we discover, or an individual is able to show us, that it is inaccurate, incomplete or out of date.

If an individual asks us to correct his or her personal information and we do not agree that it is inaccurate, incomplete or out of date, we will explain our refusal to correct the information. In these circumstances, if an individual asks we will take reasonable steps to keep a statement with the record that the individual regards the information as inaccurate or out-of-date.

7. NPP 7 - Identifiers

Privacy Principle

We will generally only adopt, use or disclose Commonwealth Government identifiers where permitted to do so.

What Does This Mean?

A Commonwealth Government identifier is a number or a word, or a combination of numbers and letters assigned by an agency to identify an individual uniquely for the agency's purposes. For example, Medicare and pension numbers are identifiers. It does not include ARBN and Australian Business Numbers.

If we are required to collect a government identifier in providing our services to individuals, we will not use this number to identify the individual.

As a general rule, we will not disclose a government identifier to any other person, except as required by law or if the disclosure is requested in writing by the individual to whom the identifier pertains.

8. NPP 8 - Anonymity

Privacy Principle

*If reasonably possible, we will give others the option of dealing with us **anonymously**.*

What Does This Mean?

Where it is lawful and practicable, we will allow individuals to enter into transactions with us on an anonymous basis.

9. NPP 9 - Transborder Data Flows

Privacy Principle

*In most circumstances, we will only transfer information **overseas** either with consent or in a way which meets the requirements of this Policy.*

What Does this Mean?

Where possible, we will not transfer personal information to someone (other than the same entity or the individual who is the subject of the information) in a foreign country, unless one of the following circumstances apply:

- we reasonably believe that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the NPPs; or
- the individual has consented to the transfer of information; or
- the transfer is necessary to perform a contract between the individual and us or the individual and a third party or for the implementation of pre-contractual measures taken in response to the individual's request; or
- the transfer is for the individual's benefit, it is impractical to get consent and it is likely consent would be given; or
- we have taken reasonable steps to ensure those to whom we transfer the personal information will not hold, use or disclose it inconsistently with the National Privacy Principles.

10. NPP 10 - Sensitive Information

Privacy Principle

*We will generally obtain consent to collect **sensitive information** unless one of the exceptions in NPP 10 applies.*

What Does this Mean?

Generally, we will collect **sensitive information** with an individual's consent unless the collection is required by law or to establish, exercise or defend a legal or equitable claim; or it is necessary to prevent or lessen a serious or imminent threat to the life or health of the person who is the subject of the information.

11. Further Information

If you have any further questions about this Policy, or if you have a specific privacy issue, please contact our Privacy Compliance Officer:

Murray Short
Tel: 02 9834-6032
Email: murray.short@stclairanglican.org.au