

### **3. Privacy Policy – Uniting Church, Synod of South Australia**

---

We are an innovative, growing church proclaiming Jesus Christ, empowered by the Spirit to transform God's world. The corporate trustee and legal entity of the Uniting Church in South Australia (the "Church") is the Uniting Church in Australia Property Trust (SA). The Church is made up of three inter-related councils: Congregations (local), Presbyteries (regional) and Synod (state).

The Church conducts religious, outreach and community activities including religious services, fellowship, weddings, funerals, baptisms, counselling and caring for members of the community.

As from 21 December 2001, the Uniting Church in South Australia has made a commitment to adhere to the Privacy Act (2000), and the National Privacy Principles that are contained in the Act, listed below:

- Collection
- Use and disclosure
- Data quality
- Data security
- Openness
- Access and correction
- Identifiers
- Anonymity
- Transborder data flows
- Sensitive Information

Further information on the principles are contained within the legislation, or from the Privacy Commissioner's Office.

The diverse range of activities of our Church also gives rise to numerous uses of personal information within the Church.

Personal information may be collected in a variety of ways including registration or enrolment forms, or in personal notes.

The information collected may include names, addresses, email addresses, telephone and fax numbers, medical details, family details (including spouses, children, guardians & parents' details), credit card and account numbers, and any notes taken for counselling purposes.

The Church only collects personal information which is necessary for its activities, and in particular only collects sensitive information where it is consented to by the individual, or their parent or guardian. Sensitive information is only shared where the Church has a belief that its use/disclosure is necessary to prevent threats to health, life or safety to any individual.

Personal information is not shared without the prior consent of the individual. It is not distributed to any organisation, which is not associated with the Uniting Church.

All personal information is stored in secured cupboards, and where possible in secured premises. All personal data in an electronic form is stored in secured facilities.

All paper containing personal data is disposed of either by secured paper destruction, shredding or incineration. All disks and other electronic storage devices containing personal data are destroyed when no longer in use.

Individuals may access data, which is held by the Church on themselves, by notifying the Church in writing of their request. The Church will acknowledge the request within 14 working days and arrange a time for viewing the data. Information which is out of date or incorrect will be updated upon written request, or the applicant will be notified of the reason why the information will not be updated.

The Church may send out newsletters and other information including information from different associated bodies of the Church from time to time. If an individual does not want to receive any of this type of information, they should notify their relevant congregation, presbytery, Synod or associated body of the Church in writing of their desire not to receive any further information.

## **4. An overview of the Privacy Principles**

---

In December 2000, the Federal Parliament passed the Privacy Amendment (Private Sector) Act 2000.

This legislation amended the Privacy Act 1988. The Amendment Act sets out how we should collect, use, keep, secure and disclose personal information. It also gives individuals the right to know what information an organisation holds about him or her and the right to correct it if it is wrong. The Act has ten National Privacy Principles (NPPs) under the following headings:

### **1. Collection**

Collection of personal information must be fair, lawful and not intrusive. A person must be told the church's name; the purpose of collection; and how to get access to their personal information; and what happens if the person chooses not to give the information.

### **2. Use and disclosure**

A Church should only use or disclose information for the purpose it was collected (primary purpose) unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure.

### **3. Data quality**

The Church will take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to date.

### **4. Data security**

The Church will take reasonable steps to protect the personal information it holds from misuse, loss and from unauthorised access modification or disclosure.

### **5. Openness**

The Church must have a document outlining its information handling practices and make this available to anyone who asks for it.

### **6. Access and correction**

An individual has the right to access the personal information that the Church holds about them (although there are some exceptions).

### **7. Identifiers**

The Church must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government agency (eg Tax file number, Medicare number).

### **8. Anonymity**

Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do.

### **9. Transborder data flows**

The Church can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.

### **10. Sensitive Information**

An organisation must not collect sensitive information unless the individual has consented, it is required to do so by law or the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual.