UNITING CHURCH PRIVACY POLICY

PREAMBLE

The Privacy Act (Commonwealth) has been in existence in various forms since 1988. The most recent changes have been implemented from March 12th 2014 in the Privacy Amendment (Enhancing Privacy Protection) Act 2012. This Amendment Act is a part of an overall privacy law reform process. The expectation of the Australian Information Commissioner is that all organisations will be proactive in continually assessing how well they are managing personal information in their care.

The latest amendments and, in particular, Australian Privacy Principle No. 1 contain clear directions on the required content of an organisation's Privacy Policy about how personal information is going to be managed by that organisation. This Policy is supported by a Synod Privacy Manual and the Policy should be read in conjunction with that Manual. The Manual also contains a summary of the latest Privacy Act amendments.

POLICY STATEMENT

The CoroUniting Church in South Australia (here in after referred to as the Church) is classified as an Australian Privacy Principles (APP) entity under the privacy legislation. For legislative, pastoral and missional reasons, the Church is committed to ongoing compliance and the proactive application of the 13 Australian Privacy Principles (APPs) contained within the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and any subsequent amendments to this Act and any Codes of Practice issued under this Act.

Specifically, the Church is committed to ensuring that personal information (see "Definitions and Terms") of any type is:

- only collected when justified by the primary purpose for which it is being or has been collected
- only used when its use is directly related to the primary purpose for which it was originally collected
- stored securely
- regularly reviewed for its accuracy and relevance
- only accessed, and/or released to third parties when consistent with the primary purpose for its original collection and the APP's
- not released when the APP's specifically provide exceptions to or conditions on its release
- in the custody of persons who can be trusted to uphold the spirit and substance of the APPs
- destroyed where the information no longer passes the primary purpose relevance test,

ensuring that all persons associated with the Church have a clear understanding to their rights under the legislation and good access to the Act and the APP's if required.

The policy recognises that any of the Councils of the Church will need to hold personal information for administrative, pastoral and missional purposes.

This policy commits the holders of personal information to best practice personal information management and see themselves as custodians or trustees of the information entrusted to them. Therefore the attitude of the Church towards privacy compliance is to be seen as not only a legislative but also a pastoral obligation.

The policy also recognises that from a risk management perspective, poor or complacent personal information management can place the Church at risk of broader reputational damage.
Finally, the policy recognises that good personal information management is best achieved by a sense of shared responsibility between the person providing the personal information and those who hold it in trust.

POLICY SCOPE

This policy statement is relevant to the Church's compliance with the Privacy Act (as amended) at the following sites Coro Uniting Church.

This policy statement is specifically applicable to all persons who manage databases (whether electronically or in hard copy) containing personal information for use in any administrative, pastoral or missional activity of the Church. It also has direct relevance to information released/transmitted on any social media sites.

AUSTRALIAN PRIVACY PRINCIPLES (APPs)

A complete version of the new APPs can be accessed by referring to the Synod Privacy Manual or accessing the following link http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform#APPs
The Synod Privacy Manual provides a comparative listing of the current APPs and the previous NPP's for those familiar with the previous legislation. The Manual also provides a summary of the scope of each of the new APPs for easy reference. However, readers of this policy are encouraged, wherever practical, to refer to the actual wording of the APPs in the Act rather than rely on the summary statement.

KEY DEFINITIONS AND TERMS

Definitions of key privacy terms viz. personal information, sensitive information and health information are attached as *Appendix 1*. In short, personal information is information about an individual that is not expected to be in any public domain such as White Pages. The definition of personal information has been expanded in the most recent amendments.

Sensitive and health information are two subsets of personal information that require specific attention by anyone responsible for managing personal information.

Managers of sensitive and health information are required to comprehensively familiarise themselves with the ways in which this information must be treated under the Act and, in particular, the strict guidelines surrounding the retention or release of this information to accredited agencies. Close liaison with the Synod

ACCURACY AND CORRECTION OF PERSONAL INFORMATION

The Church is committed to checking the accuracy and relevance of personal information held on a regular basis. This checking process should, wherever practical, involve the individuals who have personal information held by the Church. Any inaccurate or irrelevant personal information records should be destroyed within a reasonable time. At any time, an individual can make a request to have personal information altered or deleted and this request must be attended to within 21 days of the request. Notification of the completion of the correction must be sent to the individual involved. Wherever relevant, individuals should be given the ability to easily unsubscribe to mailing and distribution lists containing their personal information.

KEY CONTACT PERSONS RESPONSIBLE FOR PRIVACY ADVICE AND INFORMATION

Everyone connected with the Church has a responsibility for ensuring that implementation of the requirements of the privacy legislation and APP's are taken seriously. However, there are specific individuals who have a responsibility to be well informed on all privacy issues and constantly oversighting the application of this policy at all times.

Presbytery and Synod Privacy Officer

The Associate General Secretary has been appointed by the Standing Committee as the Presbytery and Synod Privacy Officer. All Presbytery and Synod Ministry Centres and managers of personal information at all sites described in "Policy Scope" paragraph above have a direct accountability to this position in relation to the implementation of APP's and ongoing compliance.

Privacy Contact Person

All CoroUniting Church sites described above under the "Policy Scope" paragraph will have a Privacy Contact Person (PCP). It is highly recommended that Church Councils and Faith Communities appoint a Privacy Contact Person (PCP) to oversight the application of the policy within their local context. The person appointed to this role needs to be committed to:

- keeping themselves up to date with privacy related matters
- have a demonstrated ability to maintain confidentiality
- upholding the spirit as well as the substance of the privacy legislation
- being part of a broader PCP information sharing network.

The key roles described above have specific responsibilities on behalf of the Church and these responsibilities are included in the Synod Privacy Manual.

SPECIFIC PRIVACY STATEMENTS RELATED TO COMMON CHURCH ACTIVITIES

The Church has made specific statements in relation to the application of the APP's in the following areas:

- Privacy and Public Prayer:
- Privacy and contact directories
- Privacy and electronic data bases
- Privacy and email protocols

These statements can be found in the Synod Privacy Manual.

Sharing of information between Councils of the Church and minimum consent wording

The Synod Privacy Officer is charged with the responsibility for the release of information to other Councils of the Church is monitored carefully. Uniting Church SA will expect that there will normally be a flow of personal information between the different activities of the Presbytery and Synod, congregations and faith

Privacy Officer is highly recommended when dealing with these issues. If there are any concerns or queries, the matter must be referred to the Synod Privacy Officer on privacy@sa.uca.org.au.

COLLECTION OF PERSONAL INFORMATION BY THE CHURCH

It is necessary for the Church to collect personal information in order to give maximum opportunity for individuals to be actively involved in and well informed about the life of the Church and its functions and activities. This collection of personal information can be for administrative, pastoral and missional purposes. The Church is committed to only holding personal information where it can be demonstrated as being necessary to achieve this involvement. Holders of personal information on behalf of the Church must be in a position to demonstrate to any person the relevance of personal information held by them at any time.

Individuals retain the right not to provide personal information or specify specific conditions for the holding of that information but must recognise that not disclosing some personal information may limit their involvement in the life of the Church.

Where personal information has been or is to be collected from unsolicited sources, the matter should be referred to the Synod Privacy Officer.

USE OF PERSONAL INFORMATION

Personal information is always to be used for the purpose for which it has been collected and, where required by the APP's, with the specific consent of the individual.
Where there is potential for the information to:

- be used for direct marketing
- contain credit information
- be classified as a Government identifier
- forwarded to an overseas organisation or individual,

the matter should be referred to the Synod Privacy Officer.

If a manager of personal information has a request to disclose personal information to a third party that does not, in their view, fit the primary purpose definition outlined above, the request should be declined or, if in doubt, the matter should be referred to the Synod Privacy Officer.

ACCESS TO PERSONAL INFORMATION

Unless personal information is:

- specified by law (Church and secular) or confidentiality arrangements,
- a specific exception under the APPs or another provision of the Act requires it to be inaccessible to individuals,

a person has the right to be aware of personal information stored about them, by the Church.

DISCLOSURE OF PERSONAL INFORMATION

The Church may disclose personal information where:

- it is consistent with the primary purpose of the collection of the information, or
- required or authorised by law, or
- a specific consent to the disclosure has been received from an individual.

communities unless an individual specifies otherwise. However Synod Privacy Officer retains absolute discretion as to whether personal information requested by another UCA Synod or an activity of Assembly will be released and, if so, any conditions on its release.
This is the rationale for the minimum Uniting Church SA consent wording being:
"This information has been collected for the primary purpose of communication and correspondence related to activities conducted by the Presbytery and Synod of SA. It may also be used in relation to any authorised activities of other Synods or the Assembly of the Uniting Church in Australia."

Organisers of particular activities/events can choose to use a consent wording that relates more specifically to the reason for collection of personal information e.g. KCO registration forms.

DIFFERENT FORMS OF CONSENT

Individuals giving consent to having their personal information collected, stored and used for the primary purpose can be asked to provide one of two types of consent:

- Opt in – this consent requires the specific authority of an individual to have their information collected.
- Opt out – this consent is a default position in that, unless the organisation is advised by the individual to remove personal information, the information will continue to be stored.

The Church's policy is that for the first time entry of an individual's personal information on any data base or recording system, an "opt in" process must be used and the accompanying consent form stored securely. A continuation of the "opt in" process is strongly recommended for regular events such as annual registration processes to ensure changes of personal information since the last registration process are captured. However in situations where a periodic review of the accuracy of personal information being held on data bases and other personal information storage mechanisms and where using an "opt in" process is impractical or unreasonable, putting an "opt out" option to individuals is acceptable.

COMPLAINTS PROCESSES

An individual involved with the life of the Church can register a complaint about an alleged breach of the APPs. The Church's preferred process is to attempt to resolve these issues internally by having the complaint mediated by the PCP or if necessary, the Synod Privacy Officer. However individuals can, at any time, access the provisions of the Act in relation to complaint resolution processes and address their complaint to the Office of the Australian Information Commissioner, GPO Box 5218, Sydney NSW 2001 or email enquiries@oaic.gov.au

POWERS OF THE AUSTRALIAN INFORMATION COMMISSIONER

The Church acknowledges that the Australian Information Commissioner has specific powers under the Act including the ability to:

- Recognise external dispute resolution schemes as a way of handling privacy related complaints
- Accept enforceable undertakings
- Seek civil penalties in the case of serious or repeated breaches of privacy
- Conduct assessments of the privacy performance of the Church

DISSEMINATION AND ACCESSIBILITY OF THIS POLICY

The Church's Privacy Policy will be available in printed form upon request. Alternatively, the Privacy Contact Person can be contacted during business hours on phone and/or email to answer any queries relating to this policy.

All custodians of personal information for Presbytery and Synod entities and activities, congregations and faith communities should ensure that this policy is made widely and readily available at every opportunity, including prominently displaying a hard copy of the policy in public areas.

Adopted by Rex Greenwood **Council** Chair **DATE** 16/10/18

KEY PRIVACY ACT DFINITIONS AND TERMS

Personal information means:

information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Sensitive information means:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

Health information means:

(a) information or an opinion about:

(i) the health or a disability (at any time) of an individual; or

(ii) an individual's expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual;

that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

(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