

The Uniting Church in Australia

Assembly – Finance and Administration Manual

Section 6 – Governance Policies

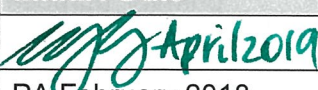
(6.6) Privacy Compliance Policy

Document History

Version	Date	Author	Comment
1.0	30 June 2011	R Groves	Approved by AFARC 19 July 2011
2.0	February 2018	J Harris / L Iosifidis	Updates as per AFARC review

Approval and Distribution

The following table lists the approvals for this document.

Name / Position / Committee	Approval	Initial / Date
Colleen Geyer, Assembly General Secretary	Supported	 April 2019
AFARC	Approved	PA February 2018

Overarching Policy Framework

This Policy is to be read in conjunction with Section 6 Governance Policies – Introduction. This sets out the Assembly Business Units to which this Policy applies, together with the Scope of the Policy and overarching Principles, Policies, Procedures and Guidelines.

Context and Background

The Privacy Amendment (Private Sector) Act No 155 of 2000 came into effect on 22nd December 2001 and requires private sector organisations, such as the Uniting Church in Australia, to develop a published privacy policy outlining how personal information is handled and managed. The Privacy Amendment (Notifiable Data Breaches) Act 2017 is effective from 22 February 2018.

While the Uniting Church is structured as a national church, administratively much of the work of oversight and administration is undertaken by the six Synods. Consequently each Synod has produced its own privacy policy and these can be found on each of the Synod websites.

The Assembly has associated with it a number of national agencies, committees, working groups, forums and task groups which, for the purpose of this privacy compliance policy, will all be referred to as the “Assembly” or “Assembly Agencies”. The work of the various Assembly Agencies is broad ranging, and the process to develop and implement an appropriate published policy to address the specific needs of each agency would be complex and cumbersome. Therefore, the Assembly has published a Privacy Policy, available to the public, which is the basic standard to which all Assembly Agencies must adhere. The Assembly website, and each website for an Assembly Agency, must display a Privacy Policy on any website for which they are responsible.

Definitions and Acronyms

AFARC	Assembly Finance, Audit and Risk Committee
ASC	Assembly Standing Committee
APP	Australian Privacy Principles
UCA	Uniting Church in Australia

Governance Policy Statement – Privacy Compliance Policy

This policy has been adopted by the Assembly in order to comply with the requirements of the Privacy Amendment (Private Sector) Act No 155 of 2000. The policy should be read together with the Australian Privacy Principles (APPs) set out in the Privacy Act. A copy of the APPs is available on the Australian Privacy Commissioner's Website. (<http://www.privacy.gov.au/>).

The Privacy Compliance Policy is covered in the following dot-points:

- In the policy, a reference to:
 - “Church” means The Uniting Church in Australia; and
 - “Assembly” means the National Assembly (national council) of the Church;
- The Assembly will comply with the APPs and related legislation. If there is any inconsistency between this policy and the APPs, then the APPs prevail.
- Subject to the following points, the Assembly will only use personal information for the primary purpose for which it is collected. In most cases, the purpose will relate to the spiritual, pastoral, social, educational and administrative functions of the Assembly.
- Those functions of the Assembly include maintaining personal information for the purpose of analysing the role of the Church in society and recording the family histories of its members. The information may be disclosed to scholars studying the Church and to relatives of the particular Church members about whom information is held.
- The Assembly will only use personal information about an individual for a secondary purpose (i.e. something beyond the scope of the primary purpose) if that individual has consented or the use is otherwise permitted by the APPs.
- The Assembly will take reasonable steps to keep personal information secure and will, subject to the APPs, comply with any request from a person to correct or remove his or her information. The Assembly has a Privacy Officer who is responsible for storing, correcting and giving people access to personal information collected about them. The Assembly may charge fees for access to personal information.
- Personal information collected by the Assembly may be sensitive information for the purpose of the APPs (e.g. information about a person's religious beliefs). As a non-profit organisation, the Assembly is permitted to collect sensitive information without a person's express consent. However, the Assembly will endeavour to seek consent from a person if sensitive information is sought for something other than the primary functions of the Assembly described above.
- The operating procedures (whether or not they are formalised in a manual) of the Assembly will comply with this policy and the APPs.
- The Assembly's Privacy Officer is empowered to receive and deal with any complaint that the Assembly has not complied with this Privacy Compliance Policy, the published Privacy Policy or the APPs. The requirements of the Privacy Amendment (Notifiable Data

Breaches) Act 2017 will be followed to investigate and report on any data breaches. If a breach has been found to have occurred, this must be reported immediately to the Assembly General Secretary and AFARC.

Any questions regarding this Privacy Compliance Policy should be referred to the Assembly's Privacy Officer.

In order for managers and staff to be reminded of the requirements of the Privacy legislation, the National Director – Strategic Finance and Administration will arrange for an annual update for all staff.

Security

The Assembly will use reasonable administrative, technical, personal and physical measures to safeguard personally identifiable information in its possession against loss, theft, unauthorised use, disclosure or modification. This applies to all data, including information provided for fundraising. However, no data transmission over the internet can be guaranteed to be totally secure.

The requirements set out in the Information Security Policy, which covers Assembly, must be observed to maintain data security.

Privacy Officer

Any questions regarding this Privacy Compliance Policy and the published Privacy Policy should be referred to the Assembly's Privacy Officer. The Privacy Officer is empowered to receive and deal with any complaint that the Assembly has not complied with this Privacy Compliance Policy, the published Privacy Policy or the Australian Privacy Principles. The Assembly's Privacy Officer is:

National Director – Strategic Finance and Administration
Uniting Church in Australia (Assembly)
Email: privacyofficer@nat.uca.org.au
Telephone: (02) 8267 4229
Location: Level 10, 222 Pitt Street Sydney NSW 2000
Post: PO Box A2266 Sydney South NSW 1235

Further Information and Guidelines

The Appendix contains additional information that applies as Policy Guidance to those Assembly Agencies and Business Units for which annual accounts are prepared by the Assembly's Accounting Unit. The Appendix may be of assistance to other Assembly Agencies or Business Units.

Access to Relevant Reference Material

The published Privacy Policy is available on the Assembly's website at:

http://assembly.uca.org.au/images/PDF/Assembly_Privacy_Policy.pdf

Policy Owner

National Director – Strategic Finance and Administration

Appendix – Policy Guidance

The Appendix contains additional information that applies as Policy Guidance to those Assembly Agencies and Business Units for which annual accounts are prepared by the Assembly's Accounting Unit, namely:

- Frontier Services
- Uniting Aboriginal and Islander Christian Congress (UAICC);
- UnitingCare Australia;
- UnitingWorld; and
- The Assembly Fund.

All Statutory Requirements relating to records must be observed. In particular, retention periods relating to personnel files and other documents must be followed.

The Privacy Compliance Policy and published Privacy Policy identify the Assembly's Privacy Officer and how to contact him or her. The Privacy Officer will undertake a regular review of all issues relating to privacy to ensure that the Policy and Procedures reflect any changes in legislation or practice.

In particular, the following checks will be undertaken as deemed necessary and no less than annually by the Privacy Officer:

- review any changes to legislation that may impact on privacy requirements;
- review the Australian Privacy Principles (APPs) set out in the Privacy Act to ensure that the principles are being followed;
- review each website for the Assembly and its Agencies to ensure that each website displays an appropriate published Privacy Policy for the particular website; and
- satisfy himself or herself that each website for the Assembly and its Agencies is responding appropriately to any privacy issues raised through the website or in respect of the website.

The Privacy Officer will conduct a rolling review to ensure that:

- information is only being collected by the Assembly when necessary;
- people are informed as to what personal information is being collected about them, and how it will be used;
- people are being given access to their own personal information held by the Assembly if they request it;
- personal information held is accurate, securely retained by the Assembly, kept up-to-date, and not disclosed to other people without the consent of the individual concerned;
- Statutory Requirements relating to the retention of records are being observed;
- information is no longer retained once it becomes unnecessary;
- personal information that is no longer needed by the Assembly is shredded, pulped, destroyed or permanently and securely deleted from computer systems;
- personal information obtained by the Assembly is used only for the primary purpose for which it is collected; and
- a report in outline is given to the Assembly General Secretary regarding any requests or complaints relating to privacy.

If the Privacy Officer suspects or is advised of a potential eligible data breach, an investigation must be carried out within 30 days as required by the Privacy Amendment (Notifiable Data Breaches) Act 2017. (For an eligible data breach to occur, the risk of serious harm occurring must be more probable than not). If the breach has occurred, the communications required under the Act to those affected or at risk must take place, with a copy of the communication to the Office of the Australia Information Commissioner.

If a breach has been found to have occurred, this must be reported immediately to the Assembly General Secretary and AFARC.

In order for managers and staff to be reminded of the requirements of the Privacy legislation, the National Director – Strategic Finance and Administration will arrange for an annual update for all staff .

