

AUSTRALIAN LUTHERAN WORLD SERVICE

PRIVACY POLICY

The Privacy Act

The Privacy Amendment Act 2000 (Commonwealth) amends the Privacy Act 1988 to include the regulation of private sector organisations and the systems used by these organisations to handle 'personal information'.

The Act details how businesses and organisations must manage personal information of customers. It regulates what personal information can be kept, in addition to how businesses collect, use, secure and disclose that information.

Individuals will have the right to know **why** an organisation is collecting their personal information, **what** information it holds about them, how it will **use** the information, and who else will **get** the information.

Individuals will also have the right to verify that personal information held by an organisation is accurate and may complain to the Privacy Officer and/or Privacy Commissioner if they think their information is not being handled correctly.

The Privacy Act and ALWS

ALWS is an auxiliary of the Lutheran Church of Australia. Under the Privacy Act, an entity that is related to another entity will be able to share and transfer personal information. However, ALWS and the LCA must still comply with the National Privacy Principles (NPP) in relation to the shared personal information. This means that ALWS must comply with the Privacy Act, in order that movement of information within the LCA can take place. This is particularly important for movement of details between ALWS and congregations (for example, donor addresses when forwarding receipts, collation of Appeal returns by Treasurers that may include information such as credit card details).

Information held by Australian Lutheran World Service

Personal information that is held by Australian Lutheran World Service includes personal and sensitive information about:

- Donors, who almost exclusively are members of LCA congregations
- staff, job applicants, volunteers and contractors
- Loan applicants and borrowers

Personal and sensitive information may be gathered by way of forms, email, telephone, face to face meetings and interviews.

What is Personal and Sensitive Information?

Personal information is basically information or an opinion that allows someone to identify the individual that the information or opinion is about. Within ALWS, personal information is likely to be collected on donors, employees, prospective employees, volunteers, board members and loan applicants. This information could include:

- name
- address
- date of birth and age
- country of birth and nationality
- telephone numbers and email addresses
- details of next of kin
- emergency contact numbers

The use of personal information refers to the handling of personal information within ALWS and the LCA including 'the inclusion of information in a publication'.

Sensitive Information is personal information about an individual's race or ethnic origin, political opinions, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences, criminal record or health information.

Sensitive information must be treated with additional care. Within ALWS, sensitive information will only be collected for employment-related purposes. It is not the policy of ALWS to seek sensitive information from donors or loan applicants.

To the extent sensitive information is collected, it will be used only for the purpose for which it is provided, unless law allows the disclosure of such information.

Use of Information

ALWS uses personal information it collects for the primary purpose for which it is collected, and for secondary purposes reasonably expected to be related to the primary purpose. The information may also be used for purposes for which consent has been gained.

The primary purposes for the collection of information are that:

- ALWS may contact donors and prospective donors, interact with them, and provide relevant information;
- appropriate people and administrative sections within the Church (Boards, Committees, Pastors, Treasurers) can be contacted;
- ALWS can effectively and efficiently administer its human resources (employment processes and appraisals).
- ALWS can exercise due diligence in the distribution of economic resources (loans and grants)

Information that is collected about volunteers assists ALWS to properly assess the capacity and appropriateness of volunteers and staff and to help it to meet duty of care requirements.

Personal information which is obtained in relation to employees, job applicants, and contractors is used to:

- satisfy legal requirements;
- administer contracts;
- provide insurance cover.

Disclosure of personal information

Personal information may be disclosed to:

- LCA Officials, Boards and Committees of the LCA (although the circumstances for sharing of such information would be very limited);
- Pastors and Congregational Treasurers;
- Outsourced service providers who manage services provided to donors;
- ALWS professional advisers, including the ALWS auditors;
- anyone the provider authorises to receive it
- government and regulatory authorities and other authorities, as required or authorised by law.

The Privacy Officer

The ALWS Privacy Officer will be the LCA Secretary. This person is the first point of contact in the LCA when privacy issues arise. The Privacy Officer is responsible for ensuring the ALWS's privacy policy and procedures are fully implemented and working effectively.

The duties of the Privacy Officer, or his/her delegated authority, are to:

- promote the privacy plan to all relevant parties within ALWS;
- familiarise ALWS staff and Board with the NPP;
- coordinate and implement the privacy policy; and
- ensure a privacy audit is conducted within ALWS.

Update of Personal Information

ALWS endeavours to maintain personal information so that it is kept up-to-date, complete and accurate. A person may update personal information by contacting Australian Lutheran World Service which holds the information, during office hours.

Complaints Process

The Privacy Officer will:

- identify (and address) any systemic or ongoing compliance problems;
- increase donor confidence in the ALWS's privacy procedures;
- build a good reputation of ALWS; and
- address complaints quickly and effectively.

Any person who believes their personal information has been inappropriately handled by ALWS may lodge a complaint with the Privacy Officer. This complaint must be in written form and clearly identify the circumstances surrounding the alleged inappropriate handling and any remedy sought. There is no prescribed form for this purpose.

If that person is dissatisfied with the handling of the complaint by the Privacy Officer or if, due to the sensitive nature of the complaint, it is inappropriate to submit the complaint to the Privacy Officer in the first instance, the matter may be referred directly to the Privacy Commissioner. The Privacy Commissioner may then investigate the complaint.

The Privacy Commissioner has discretion to instigate an investigation into any interference with privacy even if no complaint has been lodged by any party involved.

The Privacy Commissioner is empowered to order that ALWS redress any loss or damages to the aggrieved member. As a legal process, failure to comply with these directions may result in the matter being referred to the Federal Courts.

Although court action may be an end result, the complaints process emphasises a preference to resolution through mediation and conciliation.

Accessing personal information

Persons are entitled to access and examine personal information relating to them that is held by ALWS. Requests to access personal information must be addressed to the ALWS Executive Secretary.

If, upon examination of the personal information, any person identifies information that is inaccurate, incomplete or out-of-date, that person should contact the Privacy Officer with a request that the information be corrected. If the inaccuracy is established, ALWS must take reasonable steps to correct and/or update that information.

If the person or ALWS disagrees as to the accuracy of the personal information, the person can request that a statement outlining the perceived discrepancies be associated and kept with the relevant information. ALWS must take reasonable steps to comply with any such request.

Security of Personal Information

ALWS has put in place measures to protect personal information held by ALWS from modification, loss, unauthorised access and misuse or disclosure to unauthorised persons. Personal information is stored in locked filing cabinets and computers require password access.

Training

Staff are trained in the correct methods of dealing with personal information to ensure privacy/confidentiality. Knowledge of this policy is a critical element of that training.

Further Information

If any person requires further information about the way ALWS manages personal information, the Executive Secretary can be contacted.

PRIVACY ACT INFORMATION

Purpose of the private sector provisions

The private sector provisions aim to give people greater control over the way information about them is handled by requiring organisations to comply with ten National Privacy Principles (NPP). The NPP set minimum standards relating to the:

- access
- collection
- correction and disclosure
- security
- storage, and
- use

of personal information.

Other provisions of the Act

Individuals have a right to:

- access information held about them
- request correction or annotation of information if it is incorrect.
- make a complaint about the manner their personal information is handled, and/or
- receive compensation for an interference with their privacy.

Private Sector Provisions

The private sector provisions apply to organisations (including not-for-profit organisations) in the private sector. An *organisation* includes:

- an individual
- a body corporate
- a partnership
- any other unincorporated association, or
- a trust.

A *related body corporate* is defined in section 50 of the Corporations Act 2001 (Cth) to mean that where a body corporate is:

- a holding company of another body corporate;
- a subsidiary of another body corporate; or
- a subsidiary of a holding company of another body corporate;
- the first mentioned body and the other body are related to each other.

ALWS's relationship to the LCA falls within the definition described in section 50 of the Act.

The Act applies to organisations with an annual turnover of more than \$3 million and to all health service providers.

Businesses with an annual turnover of \$3 million or less are exempt for the new laws unless one of the following applies to the business:

- it is related to another business that has an annual turn of over more than \$3 million;
- it provides a health service and holds health records other than an employee record;
- it discloses personal information for a benefit service or advantage;
- it provides someone else with a benefit, service or advantage to collect personal information; or
- it is a contracted service provider for a commonwealth contract.

The Privacy Act also exempts from its coverage:

- acts or practices in relation to employee records of an individual if the act or practice directly relates to a current or former employment relationship between the employer and the individual.

NATIONAL PRIVACY PRINCIPLES

NPP	TOPIC	WHAT INFORMATION THE NP P APPLIES TO
NPP 1	Collection	Only applies to information collected after 21 December 2001
NPP 2	Use and disclosure	Only applies to information collected after 21 December 2001
NPP 3	Date quality and collection	As it applies to collection only applies to information collected after 21 December 2001
NPP 4	Data security	Applies regardless of when information is collected
NPP 5	Privacy Policies and openness	Applies regardless of when information was collected
NPP 6	Access and correction	If information already held is not used or disclosed it only applies to information collected after 21 December 2001. But if information already held is used or disclosed after commencement then rights of access and correction apply unless <ul style="list-style-type: none"> • there is unreasonable administrative burden or • the organisation is caused unreasonable expense.
NPP 7	Commonwealth Government identifiers	Applies regardless of when information collected
NPP 8	Anonymity	Only applies to information collected after 21 December 2001
NPP 9	Transborder data flow	Applies regardless of when information collected
NPP 10	Collection of sensitive information	Only applies to information collected after 21 December 2001

NPP 1 – Collection of Information

If an organisation cannot effectively pursue a legitimate function or activity without collecting personal information, it would ordinarily be considered necessary for that function or activity.

The collection of the information must be lawful.

The individual should be informed at or before the time of collection of information.

Individuals need to be informed about the purpose of the collection of any information. This can be reasonably general as long as the description is adequate to ensure that the individual is aware of that the organisation is going to do with information about them.

Organisations must take reasonable steps to tell the individual about any law that requires the individual to provide, or the organisation to collect, personal information in particular situations.

Aim to ensure that any individual collected about an individual is collected only from the individual.

Where does ALWS collect information?

Personal information from donation slips, ALWS brochures, LCA sources (eg Yearbook)

Loan application forms

NPP 2 – Use and Disclosure

The use of primary information can be determined by the context in which the information is given by the individual to the organisation. Information provided by an individual must always be for a particular purpose.

If personal information is sensitive information the use or disclosure must be directly related to the primary purpose of collection. There must be a stronger connection between the use or disclosure and the primary purpose for collection.

Points to be considered:

The context in which the personal information is being collected

The reasonable expectation of the individual whose information it is;

The form and content of information the organisation has given about why it is collecting the individual's information

How personal, confidential or sensitive the information is; and any duties of care of other professional obligations an organisation might have.

The Privacy Act does not override specific legal obligations relating to use of disclosure of personal information.

Organisations may disclose personal information where it reasonably believes this is reasonably necessary for a range of functions or activities carried out by, or on behalf of, an enforcement body.

Unless the law prohibits it, the organisation must make a written note of such a use or disclosure.

Secondary use and disclosure with consent allows organisations to use or disclose personal information for a secondary purpose if it has the individual's consent.

NPP 3 Data Quality

Organisations need to take reasonable steps to confirm the accuracy, completeness and currency of the personal information they hold at the time they collect, use or disclose it.

Organisations may be obliged to correct personal information should an individual to whom the information relates establish that it is not accurate, complete or up-to-date.

NPP 4 – Data Security

Organisations must ensure that reasonable steps are taken to protect personal information it holds from misuse and loss, and from unauthorised access, modification or disclosure.

Security measures could include:

- Physical security – measures to prevent unauthorised entry to premises, systems to detect unauthorised access and secure containers for storing paper-based personal information
- Computer and network security - measures to protect computer systems and networks for storing, processing and transmitting personal information from unauthorised access, modification and disclosure
- Communications security – preventing unauthorised intrusion into computer networks; and
- Personnel security – adopting procedural and personnel measures for limiting access to personal information by authorised staff for approved purposes and controls to minimise security risks to an organisation's IT systems.

Reasonable steps must be taken to destroy or permanently de-identify personal information if it is no longer needed for any purpose under NPP 2. Reasonable steps include shredding, pulping or disintegration of paper. De-identification involves the removal of any information by which an individual may be identified.

NPP 5 – Openness

A policy document should outline whether an organisation is bound by the NPP.

Any exemptions under the Privacy Act that apply to the personal information the organisation holds or to any of its acts or practices; and that an individual can get more information on request about the way the organisation manages the personal information it holds.

The organisation must make the document available to anyone who asks for it.

Information regarding personal information management policies could be distributed by:

- Displaying the organisation's privacy policy on a sign;
- Provision in a printout or pamphlet that is handed out on request;
- A privacy policy could be put on a web site, either on a home page or on a prominent and accessible link from the home page.

Information made available in this manner could include:

- The kind of personal information the organisation holds;
- The main purposes for which the organisation holds the information;
- Whether it contracts out services that involve the disclosure of personal information;
- How the individual may complain about a breach of privacy including a contact number in the organisation
- The organisation's contact details; and
- How the organisation handles requests for access to personal information.

NPP 6 – Access and Correction

Individuals have the right to access all personal information that an organisation holds about them.

Individuals could be given access by allowing them to inspect records, take notes or by giving them a photocopy or printout.

Organisations are required to take reasonable steps to correct information about an individual where that information is not accurate, up-to-date and complete. Where an organisation and individual are unable to agree about whether personal information is accurate, up-to-date and complete, the

organisation must, at the request of the individual take reasonable steps to associate with the personal information the individual's claim that it is not accurate, complete and up-to-date.

NPP 7 – Identifiers

This principle ensures that the increasing use of Commonwealth government identification does not lead to a de facto system of universal identity numbers, and to prevent any loss of privacy from the combination and re-combination of the data.

Organisations are not permitted to adopt a government identity number as if it were its own.

Organisations may use or disclose a Commonwealth Government identifier to those in which such use or disclosure is:

- Necessary for the organisation to fulfil its obligations to the agency that assigned the identifier to the individual, or
- In the interest of health or safety or authorised or required by or under law, or in certain other public interests; or
- Under regulations that allow use or disclosure of the identifier by a certain organisation in certain circumstances.

NPP 8 – Anonymity

Unless there is a good practical or legal reason to require identification, organisations must give people the option to operate anonymously.

NPP 9 – Transborder data flows

Organisations are prevented from disclosing personal information to someone in a foreign country that is not subject to a comparable information privacy scheme, except where it has the individual's consent or some other circumstances where:

- the transfer is for the benefit of the individual and the organisation can show grounds for a belief that if it were practicable to obtain consent the individual would be likely to give it; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party.

Transfers of personal information outside Australia by an organisation to another part of the same organisation, or to the individual concerned is not prevented.

NPP 10 – Collection of Sensitive Information

Organisations need clear evidence that an individual has consented to the collection of sensitive information.

AUSTRALIAN LUTHERAN WORLD SERVICE

PRIVACY POLICY STATEMENT

Australian Lutheran World Service understands the importance of protecting privacy and is committed to complying with the Privacy Act 1988 and the National Privacy Principles. A copy of the Privacy Policy is available on request.

Information held by the Lutheran Church of Australia

Personal information which is held by Australian Lutheran World Service includes personal and sensitive information about:

- donors and prospective donors
- staff, job applicants, volunteers and contractors
- loan applicants

Personal information may be gathered by way of forms, email, telephone, face-to-face meetings and interviews.

Use of Information

Personal information is collected so that:

- ALWS may contact you, interact with you, and provide relevant information to you;
- ALWS can contact appropriate people and administrative sections within the Church (LCA Officials, Pastors, Treasurers);
- ALWS can effectively and efficiently administer its human resources (employment processes and appraisals).
- ALWS can exercise due diligence in the distribution of economic resources (loans and grants)

Security of Information

ALWS takes all reasonable steps to ensure that personal information is secure. All computers have password access and personal information is kept in locked storage.

All employees and volunteers with access to personal information are trained in the need for and are required to respect the confidentiality of all personal information and the privacy of individuals.

Complaints about a breach of privacy

Complaints about any breach in maintaining the privacy of an individual should be addressed to the LCA Secretary.

Requests for access to personal information

The Privacy Act gives you the right to access personal information held about you and you can ask for the information to be corrected if it is inaccurate. More information is set out in the Privacy Policy. Any request for access to personal information should be directed in the first instance to the ALWS Executive Secretary.

IMPLEMENTATION OF THE POLICY

ALWS has conducted a Privacy Audit to ensure compliance with the Privacy Act and National Privacy Principles (NPP).

ALWS is not required to appoint a Privacy Officer. The LCA Secretary will be the Privacy Officer for the ALWS. ALWS will distribute the ALWS Policy Statement through its newsletter, and publish it on the Web site.

The ALWS Executive Secretary will be responsible to ensure ALWS complies with the Privacy Policy.

- A copy of the ALWS Privacy Policy will be held in the ALWS Manual and made available to any person who requests the policy.
- A Standard Collection Notice will be included on or with any documents used to collect personal information.

Standard Collection Notice

A Standard Collection Notice would cover the majority of personal information collection situations by ALWS. This Notice will be included on or with any requests for information. A suggested Standard Collection Notice follows:

Standard Collection Notice

1. ALWS collects personal information about you in order to process your requests and/or contributions.
2. We may include your contact details in donor lists to inform you about our work and of opportunities to support it. If you do not agree to this you must advise us immediately.
3. Some of the information we collect is to satisfy ALWS's legal obligations.

PRIVACY AUDIT Questionnaire

What personal information does ALWS collect?

- Donor details that includes name, address, contact numbers, credit card and bank account information
- Employment records
- Loan Applicant details that includes name, address, nationality, contact numbers and personal financial information.

How is the information collected?

- Over the phone, email, personally, donation slips, application forms, brochures.

Where and how is the information stored?

- Hardcopy information is held on file in filing cabinets
- Donor and borrower information is held on two networked computers.

Who within ALWS has access to the personal information it holds and who actually needs to have access to the information?

- ALWS has four staff, all of whom have and require access to the personal information to enable them to carry out their normal duties, eg receipting, correspondence to provide information and solicit further support as necessary
- The ALWS auditor will also have access to personal information strictly for audit-related purposes. His/her request for information will be channelled through the ALWS Executive Secretary.

Are there procedures in place in relation to the handling of sensitive personal information?

- Sensitive personal information is only collected for the purposes of filling job vacancies and employment-related matters. This information is restricted to the Executive Secretary, and Interview Panels

Are there adequate measures to protect the personal information held from unauthorised access?

- All hardcopy information is secured in locked cabinets or the office safe. Keys are held only by the four ALWS staff. Computers are limited to the four staff who have password access.

Why is the personal information collected? Is the information needed for a function or activity ALWS?

- Personal information is collected to enable ALWS to fulfil its objectives which include fundraising initiatives within its constituency, and servicing of that constituency through provision of receipts to donors, dissemination of information about the work of ALWS, and encouraging support for the work of ALWS. ALWS also provides support to displaced people arriving in Australia through two revolving loan funds, which require sufficient information about them to assess their capacity to meet their commitments to ALWS and/or confirm their eligibility for assistance.

Do donors know the information is being collected?

- Yes, currently ALWS's only source of information is provided by donors in the form of completed donation slips, ALWS brochures or other similar means.

How is the information used?

- Preparing and issuing receipts to donors, adding to a mailing list for future correspondence, direct contact where necessary to obtain specific information that will enable ALWS to fulfil its obligations, assessment of loan applications.

Are all intended uses of the information disclosed to donors?

- Standard collection forms will be used to disclose use of information to donors.

Is personal information relevant, accurate, complete and up to date?

- ALWS only collects data that is relevant to its ongoing operations. Any advised changes to personal information are amended as quickly as possible to ensure information is complete and up to date.

Have you put into place a process to identify and remove information that is out-of-date, inaccurate or no longer relevant to the operations of ALWS?

- The ALWS Office Secretary is responsible for amending records that are advised through LCA publications such as The Lutheran.
- The ALWS newsletter encloses a donation slip that has provision to enable donors to advise changes to their personal information.
- The ALWS “secondary mailing list” only contains names and addresses of donors and is only activated for special appeals. Any returned mail will result in appropriate noting of ALWS records.

Do you have procedures for the safe and discreet destruction of these records?

- ALWS shreds obsolete hardcopy records and deletes computer data as appropriate

Is the information given to anyone outside ALWS and the LCA?

- The ALWS auditor for audit purposes related to verifying recording of income and assessing the management of the ALWS loan portfolio.

Is any information transferred overseas?

- Only in regard to persons seeking employment with LWF, which in all cases is done at the request of the prospective employee.

Have you trained the appropriate people in the correct procedures and requirements in relation to the National Privacy Principles and the Privacy Policy of ALWS?

- ALWS staff have been trained in the correct procedures and requirements, and have a copy of the NPP and Privacy Policy in their copies of the ALWS Manual.