Privacy Policy & Procedure

1. Introduction

Lutheran Disability Services (LDS) will actively protect the privacy of everyone involved with its functions and services. The Board, CEO and employees will carry out this objective by ensuring that information collected by LDS is shared with others only when:

- the Australian Privacy Principles are met, and
- it is in the interest of the person, and
- only when the appropriate consents are given, and
- only on a 'need to know' basis.

2. Purpose

The purpose of this Policy & Procedure is to document how LDS will comply with:

1. The Australian Privacy Principles, as set out in the Privacy Act 1988, and amended by:
    a. The Privacy Amendment (Private Sector) Act 2000 (Cth)and
    b. The Privacy Amendment (Enhancing Privacy Protection) Act 2012.
2. The SA Government Information Sharing Guidelines (ISG) Policy
3. The NDIS Code of Conduct; Guidance for Service Providers.

3. Scope

This Policy & Procedure applies to all LDS employees – full or part time, contract, casual or volunteers, consultants, people working on our premises and homes.

4. Definitions

Access	This involves LDS giving an individual/ advocate information about the individual. This may include inspecting personal information held by LDS or providing a copy of the information.
Collection	LDS collects personal information if it gathers, acquires or obtains personal information from any source or by any means. This includes information not requested, or information obtained by accident.
Disclosure	In general terms, information is disclosed when LDS releases information to others. Disclosure does not include giving information to an individual/ advocate about the individual – that is Access.
Organisation	An individual, body corporate, partnership, unincorporated association or a trust.
Personal Information	Is information or opinion (including any forming part of a database) relating to an individual, which may be provided to LDS, as part of its support activities, either in material form or not, and whether true or

	not. Such information may personally identify an individual or make a person's identity apparent. Personal information also includes metadata and behavioural data which may identify individuals.
Purpose	Is the reason for which LDS collects personal information
Record	A document, database (however kept), photograph or other pictorial representation of a person.
Sensitive Information	Refers to information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual practices, criminal record or health information, including any disability.
Use	Refers to the handling and managing of information within LDS, including use of the information in a publication.

5. Policy

It is LDS Policy to follow the Australian Privacy Principles (***Refer to Attachment 1***), as set out in the Privacy Act 1988 (Amended by the Privacy Amendment (Private Sector) Act 2000) and the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

LDS recognises the importance of protecting personal information, which it may need to collect from its employees, clients, volunteers and those associated with the service and will take all reasonable steps in order to comply with the Privacy Act and protect the privacy of the personal information that it holds.

In addition, it is LDS Policy to follow the *SA Government's Information Sharing Guidelines for promoting safety and wellbeing (ISG)* issued 2013 which outlines conditions under which information can be shared across agencies. See: Information-Sharing-Guidelines.pdf (dpc.sa.gov.au)

It is also LDS Policy that:

- before any private information held by LDS is released to a third party by LDS, the written and informed consent of the person must be obtained
- individuals may make a request to access to their own personal information
- if an individual believes that LDS has breached their privacy under any aspect of this Policy they firstly should lodge a complaint by referring to the *Complaints Handling Procedure*
- all employees, contractors and volunteers are required to sign a confidentiality clause which is included in their Employment Contract, prior to commencement of working with LDS.

6. Procedure

LDS recognises the importance of protecting personal information, which it may need to collect from its employees, clients, volunteers and those associated with the service and will take all reasonable steps in order to comply with the Privacy Act and protect the privacy of the personal information that it holds.

6.1 Client Information

6.1.1 Collection and use of information

LDS may require the collection of personal information, including health information, to be able to provide appropriate accommodation and community participation support services for clients.

Therefore, LDS will only collect personal information, which is essential for the purpose for which it is required.

The collection of personal or sensitive client information requires clear, informed, and specific prior written consent from the individual or nominated advocate, family member or representative of the Public Trustee, as directed by the Guardianship Board. Refer **Consent to Collect and use Information (C01).**

The reasons for the collection of personal information include, but are not limited to:

- accommodation placement
- health management
- spiritual development
- personal development options
- improved independence
- community participation
- holidays
- referral to other necessary services and supports, or
- legal/ financial responsibilities pertinent to contractual obligations.

LDS may collect and hold personal information in order to provide exemplary accommodation and community participation support services to clients; therefore, may need to be shared for “Duty of Care” reasons within LDS, on a “need to know” basis.

LDS may also use such information to determine client satisfaction with the service.

Other forms used are Client Photograph Video Authorisation (C03), and Approval for Client Personal Spending **(C41).**

6.1.2 Disclosure of information

LDS will not disclose personal or sensitive information to a third party unless it is:

1. necessary to provide appropriate services to clients,
2. legally required and verified by government or associated bodies, or
3. authorised in writing by the individual, their nominated advocate, family member or representative of the Public Trustee, as directed by the Guardianship Board, who provided the personal information.

The form to be used is Consent to Collect and use Information (C01).

Where the person’s age, level of ability or language, causes difficulties for the person who is to give informed consent, the CEO is required to engage a suitable advocate.

However, situations may arise where information is shared without consent where:

1. it is not possible to seek consent, or
2. where seeking consent places the client or a family member at risk of anticipated serious threat to their wellbeing and/ or safety.

In such cases, employees must follow the *SA Government Information Sharing Guidelines (ISG) Policy*, and the NDIS Code of Conduct; Guidance for Service Providers. Consent must be obtained from the CEO or the Senior Client Services Manager. All details including why consent was not received must be recorded in the Client's file.

6.2 Employee Information

LDS collects personal information from employees and volunteers which is used to discharge its legal obligations to the ATO, Superannuation Funds, Safework SA and other State or Commonwealth Departments.

Permission for collecting and using this information is provided via the employee's contract of employment.

6.3 Storage, access and retention of personal & sensitive information

LDS will take all reasonable steps to protect the security of the personal information that it holds.

All personal and sensitive information collected by LDS will be stored in hard or soft copy in secure files accessible only to designated personnel.

All employees, contractors and volunteers are required to sign a confidentiality clause, which is included in their Employment Contract, prior to commencement of working with LDS.

Where personal information held by LDS is no longer required, LDS will destroy such personal information by the secure destruction or deletion of files.

6.4 Access to Information

Individuals may make a written or verbal request to access their own personal information to the Senior Client Services Manager, or the Senior Finance Manager who will ensure that access is granted within a timely manner of the request and that access is gained at no cost to the individual.

The Senior Managers may deny a request for lawful reasons.

Where a request is denied, the Senior Manager must provide the individual (or advocate) the lawful reason for the refusal in writing and the opportunity to lodge a complaint about the decision according to the grievance procedure outlined below.

6.5 Complaints for breaches of Privacy Act

If any individual believes that LDS has breached their privacy under any aspect of this Procedure they firstly should lodge a complaint by referring to the *Complaints Handling Procedure* and by submitting a complaint in writing to the Chief Operations Officer.

LDS will endeavor to resolve the issue promptly.

Should the matter not be resolved internally, the CEO must inform the complainant that they have the right to complain to the Privacy Commissioner and that advice about making a complaint can be obtained from the **Privacy Hotline ph:1300 363 992.**

6.6 Training and Awareness

All employees will receive training on privacy procedures and implications of any amendments to the Privacy Act 1988, or subsequent Acts.

7. Responsibilities

The **CEO** has the ultimate responsibility for implementing this Policy & Procedure plus ensuring awareness throughout LDS of the *SA Government's Information Sharing Guidelines for promoting safety and wellbeing (ISG),* issued 2013 and the NDIS Code of Conduct, Guidance for Service Providers.

The **Senior Finance Manager** has the responsibility to:

- ensure that there are facilities available for the safe storage of records
- communicate the Policy & Procedure to office employees and ensure it is followed
- respond quickly to any requests to access their information
- respond quickly, seriously and effectively to any complaints.
- be aware of penalties for non-compliance and enforcement powers of regulatory bodies

The **Senior Client Services Manager** has the responsibility to:

- communicate the Policy & Procedure to support workers and ensure it is followed
- ensure that this Policy is communicated to clients and their nominees/ guardians
- respond quickly to any requests to access their information
- respond quickly, seriously and effectively to any complaints.
- be aware of penalties for non-compliance and enforcement powers of regulatory bodies

Employees have a responsibility to:

- be familiar with the Privacy Policy & Procedure and follow it.

8. Legal and Other Documents

Privacy Act 1988
Privacy Amendment (Private Sector) Act 2000 (Cth)
Privacy Amendment (Enhancing Privacy Protection) Act 2012.
SA Government Information Sharing Guidelines (ISG) Policy
NDIS Code of Conduct; Guidance for Service Providers.

Attachment 1: Australian Privacy Principles

Australian Privacy Principles

In 2014, the Australian Privacy Principles (APP) replaced the previous National Privacy Principles, to regulate the handling of personal information by Australian and Norfolk Island Government agencies and some private sector organisations covered by the Privacy Act 1988.

The APPs are legally binding principles, which are the cornerstone of the privacy protection framework in the Privacy Act. The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.

They apply to most Australian Government (and Norfolk Island Government) agencies and some private sector organisations collectively referred to as APP entities and include Lutheran Disability Services.

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.