POL/BM 10 PRIVACY AND CONFIDENTIALITY POLICY

DOCUMENT CONTROL				
DOCUMENT #	VERSION	AUTHOR	AUTHORITY	REVIEW DATE
Pol/BM10	1	CEO	Board	August 2025

Policy Statement

Lifebridge Australia Ltd. (Lifebridge) is committed to protecting the privacy of individuals' personal information. Lifebridge will only collect personal, sensitive and health information that is necessary to conduct our business as an approved provider of NDIS and Aged Care Services.

Lifebridge is legally bound to comply with the obligations imposed by the Australian Government Privacy Amendment (Enhancing Privacy Protection) Act 2012, which is an amendment to the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), as well as industry specific legislation such as the Aged Care Act, the NDIS Act and their Principles.

This policy applies to all Lifebridge Representatives (employees, contractors or subcontractors, employees of a labour hire company assigned to work in our business, outworkers, apprentices or trainees, work experience students and volunteers.)

In meeting our obligations with respect to the protection of personal information we hold, all Lifebridge Representatives are required to sign a Privacy and Confidentiality Agreement and a Code of Conduct Agreement.

In meeting our obligations with respect to the privacy of our customers, we acknowledge that people with vision or hearing impairments and those of culturally and linguistically diverse people may require special consideration.

Definitions

Personal Information is 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 is a type of personal information and includes information about an individual's health (including predictive genetic information), racial or ethnic origin, political opinions, membership of a political association, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual orientation or practices, criminal record, biometric information that is to be used for certain purposes, biometric templates.

Health information is information or an opinion about the health or a disability (at any time) of an individual, an individual's expressed wishes about the future provision of health services to him or her, or a health service provided, or to be provided, to an individual that is also personal information or other personal information collected to provide, or in providing, a health service, other personal information about an individual collected in connection with the donation, or intended donation, by the individual or his or her body parts, organs or body substances or 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.

Unsolicited information is all personal information received from an individual that we did not actively seek to collect.

Employee record is a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following; the engagement, training, disciplining or resignation of the employee, the termination of the employment of the employee, the terms and conditions of employment of the employee, the employee's personal and emergency contact details, the employee's performance or conduct, the employee's hours of employment, the employee's salary or wages, the employee's membership of a professional or trade association, the employee's trade union membership, the employee's recreation, long service, sick, personal, maternity, paternity or other leave; and the employee's taxation, banking or superannuation affairs.

Scope

This policy applies to all Staff Members, Directors, Volunteers, Students and Contractors of Lifebridge Australia Ltd. For the purpose of this policy, Staff Members, Directors, Volunteers, Students and Contractors are referred to as Lifebridge Representatives.

Protocol

1. Collection of Personal Information

Lifebridge may collect personal information from our customers and their representatives, prospective customers and their representatives, external agencies and their employees, health practitioners, health providers or facilities, legal advisors, job applicants, suppliers and their employees, contractors and individuals who visit the Lifebridge Australia website or social media pages.

Lifebridge will only collect personal information if the information is necessary for one or more of our functions as an approved NDIS and Aged Care Services provider, the individual has provided their consent and collection is necessary to:

- comply with the provisions of State, Federal or Commonwealth law;
- provide data to government agencies in compliance with State, Federal or Commonwealth law;
- determine eligibility to entitlements provided under any State, Federal or Commonwealth law;
- provide appropriate services and care;
- enable contact with a nominated person regarding a customer's health status; and
- lawfully liaise with a nominated representative and to contact family if requested or needed.

There may be some instances where personal information may be collected indirectly because it is unreasonable or impractical to collect personal information directly from the individual.

The personal information Lifebridge collects will be determined by the nature of the interaction that the individual has with Lifebridge. It may include:

- Contact details such as name, address, phone numbers, email address, emergency contact details, date of birth, gender;
- Referral information from other agencies;
- Information provided at intake for prospective customers;
- Information provided at induction for prospective employees and volunteers;
- Where necessary, financial information;
- Where necessary, health information.

2. Collection of Sensitive Information

Lifebridge may also collect sensitive information and this may include information about an individual's health, racial or ethnic origin, political opinions, association memberships, religious beliefs, sexual orientation, criminal history, genetic or biometric information.

Lifebridge will not collect sensitive information (including health Information) unless the collection of that information is reasonably necessary for, or directly related to one or more of Lifebridge Australia's functions and;

- the individual has consented to the collection of this information; or
- the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or
- a permitted general situation exists to the collection of the information; or
- a permitted health situation exists in relation to the collection of the information.

At admission, individuals can identify any parties from whom they do not wish personal information accessed or to whom they do not wish personal information provided. This request will be recorded in the file of the individual and complied with to the extent permitted by law.

Some individuals may not want to provide personal information to Lifebridge Australia and in these circumstances Lifebridge may not be able to provide the appropriate care and services that the individual may require.

3. Unsolicited Information

If Lifebridge receive unsolicited personal information from an individual that we could not have obtained by lawful means, we will destroy or de-identify the information as soon as practicable and in accordance with the law.

4. Use of Personal Information

Lifebridge will use personal information collected for the purpose of providing services to our customers and to facilitate our internal business operations, which includes our customer management and rostering systems, our financial systems and our human resources functions.

The NSW and Commonwealth governments collect some personal information through Lifebridge Australia customers through the Data Exchange (DEX).

The Commonwealth and NSW governments and/or their agencies such as Safe Work NSW collect information from Lifebridge on customers when the following has occurred:

- Unexpected death of a customer;
- Serious injury to a customer;
- Allegations of misconduct; and
- A natural disaster or event.

5. Disclosure of Personal Information

Disclosure of personal information is restricted to Lifebridge Australia personnel directly involved in the support, supervision, assessment, and management of the customer, staff member or volunteer and in other circumstances as described under Protocol "Authorised Disclosure".

Personal information regarding a customer, volunteer or staff member may be disclosed:

- When valid, informed consent is obtained from the customer and/or carer, staff member or volunteer for disclosure of specific information for a specific purpose;
- When a staff member believes disclosure is necessary in the interests of public safety. In this situation, the staff member should contact the CEO or their Manager;
- Where there is an obligation under the Crimes Act 1900 to notify police about serious criminal offences (including drug trafficking, serious assaults of a physical or sexual nature or murder and manslaughter);
- Where there is an obligation under the Ombudsman Act 2974 (Part 3C) to notify a reportable offence;
- Where a subpoena has been issued;
- Where required by a State or Commonwealth funding body;
- Where there is an obligation to report a notifiable incident to a government body under the Aged Care Act 1997 or the NDIS Act 2013;
- Where there is an obligation under the Coroners Act 2009 (NSW) to notify the coroner of deaths occurring under certain conditions; and/or
- Personal information will be provided to government authorities who have specific statutory powers to demand access to this information.

In these circumstances the CEO will be responsible for responding to the subpoena promptly and will:

- Obtain the precise authority of the person requesting access, including reference to the Section of the Act under which access is authorised;
- Obtain the nature of the access requested, to ensure that only material relevant to the statutory demand is released; and
- Bring the subpoena to the attention of the organisation's solicitors and the Board if necessary.

This information will be recorded and stored in the customers', staff members', volunteers' or other relevant file.

The use and disclosure of health information for secondary purposes (For example, research or collection of data for government departments) will be in accordance with the Health Privacy Principles 10(1)(d) and 11(1)(d) related to the Health Records and Information Privacy Act 2002 (NSW).

No personal information collected at Lifebridge on staff or volunteers will be disclosed to any overseas recipients.

The CEO is the only individual authorised to divulge information related to staff members, customers or volunteers, where it is legally and ethically justified, such as in the case of a guardianship hearing. The CEO may nominate another member of the organisation to provide this information.

6. Access to Personal Information

A customer, staff member, volunteer or their nominated representative may, by means of written application to the CEO of Lifebridge Australia, request access to their personal information. The CEO, within 5 business days of receiving the request, will respond to the request made and provide access to the person's requested information in a mutually agreed format.

The application to the CEO for the request to access the record will be retained in the person's file.

A person is entitled to dissent from or add to the information kept in their file. The person's own comments will be attached, as an addendum, to the file along with an explanation of the circumstances.

7. Storage and Security of Personal Information

Lifebridge Australia is committed to keeping secure the personal information in both electronic and hard copy form from misuse, interference, loss and unauthorised access, modification and disclosure of that information.

Lifebridge will take all reasonable steps to protect the security of the personal information we hold from both internal and external threats by:

- Storing hard copy information in a secure storage area that can only be accessed by authorised Lifebridge representatives.
- Storing electronic information on secure servers that are protected by the use of firewalls and virus scanning tools to protect against unauthorised interference or access.

- Use of individual usernames and passwords when accessing personal information via Lifebridge's electronic equipment or mobile devices.
- Conducting regular internal or external audits to assess whether we have adequately complied with or implemented these measures.
- All Lifebridge representatives have signed a Privacy and Confidentiality Agreement and a Code of Conduct Agreement and are informed via Staff Updates, staff training sessions, handbooks and at induction of their obligations with regard to the Privacy Policy.
- All Lifebridge Australia office based staff have been provided with a company mobile phone and Lifebridge Australia email address for the purpose of ensuring the security of personal information.
- All Lifebridge remote workers who use their personal mobile device to access customer information are required to maintain strict password protocols and multifactor authentication processes to ensure the privacy of information.
- All Lifebridge addressed mail will only be opened by the addressee and any general mail will be opened by the receptionist and forwarded to the appropriate department. All internal mail will be sent in a sealed envelope, addressed to the individual by name.
- The anonymity of customers and/or staff members/volunteers will be maintained during case presentations, meetings, research activities and at seminars and conference presentations.

8. Promotion, Media, Website and Social Media Channels

Lifebridge may take photos, film events or ask for individual's stories and use them for promotional purposes in our marketing materials, media, website and social media channels. At all times consent must be provided by that individual for the use of their photo, film or personal information on any of Lifebridge Australia's marketing materials, media articles, website and social media channels.

When individuals access the Lifebridge website, Lifebridge may collect personal information only if that individual chooses to enter their personal information into the online Contact Us or Enquiry Form.

Lifebridge will not use or disclose personal information about an individual for the purposes of direct marketing, unless the information is collected directly and:

- The person would reasonably expect us to use or disclose their Personal Information for the purpose of direct marketing; and
- The person selects to 'opt-out' .

No information regarding a representative of Lifebridge Australia will be disclosed to the media. Requests from the media for information will be referred to the CEO who, in consultation with the Board, will determine what information, if any, will be provided. The decision will be based on consideration of:

- Consent from the relevant parties,
- Possible legal implications,
- Ramifications to relevant individual(s) and/or the organisation.

9. Quality of Personal Information

To ensure that personal information that we collect is accurate, up-to-date and complete Lifebridge will:

- Record information in a consistent format,
- Promptly add updated or new personal information to existing records,
- Regularly audit personal information to check accuracy.

10. Disposal of Personal Information

Lifebridge Australia will dispose of all personal information in a secure manner once the information is no longer required in accordance with Policy BM3G – Record and Information Management. Methods may include:

- By shredding the documentation in-house;
- By outsourcing to a confidential documentation destruction company;
- By having electronic personal records permanently deleted off databases, hard drives, devices and servers.

11. Grievance Procedure

If you wish to make a complaint about the way Lifebridge Australia have managed your personal information you may make that complaint verbally or in writing by setting out the details of your complaint to any of the following:

Lifebridge Australia Privacy Officer - 1800 043 186
Email: communications@lifebridge.org.au

Lifebridge Australia Website Feedback Form
https://www.lifebridge.org.au/feedback/

Community Services Manager - 1800 043 186
Email: Andrew.Weir@lifebridge.org.au

Chief Executive Officer - 1800 043 186
Email: Bronwyn.Mitchell@lifebridge.org.au

Staff may also lodge a complaint by completing an issue log on Projex or a Confidential Improvement Log.

Alternatively, complaints may also be referred to the Australian Information Commissioner.
The Australian Information Commissioner receives complaints under the Act. Complaints can be made online: http://www.oaic.gov.au/privacy/making-a-privacy-complaint
By phone on 1300 363 992, By fax: on +61 2 9284 9666

In writing, by addressing your letter to the Australian Information Commissioner at the:
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
OR
Office of the Australian Information Commissioner
GPO Box 2999
Canberra ACT 2601

12. How We Deal with Your Complaint

The complaint will be investigated by Lifebridge Australia in accordance with our internal procedures and processes.

The complainant may be invited to participate in a conference by the relevant Manager conducting the investigation. At the discretion of Lifebridge Australia other interested parties may also be invited to participate in the conference to discuss the nature of the complaint and attempt to resolve it. This may include the presence or participation of a support person or advocate for the complainant.

The complainant will be provided with a response to their complaint within a reasonable timeframe after completion of any investigation. This response will be in writing and will include the outcome of the investigation, any proposed action and details of the right to lodge a complaint with any relevant external organisations.

Relevant Legislation and Guidelines

- Privacy Act 1988 (amended by the Privacy Amendment (Private Sector) Act 2000)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Protected Disclosures Act 1994
- Freedom of Information Act 1989
- Privacy and Personal Information Protection Act 1998 (NSW)
- Privacy and Personal Information Regulation 2009 (NSW)
- Convention of rights for person with a disability (United Nations 2018)
- The National Disability Insurance Scheme (NDIS) Act 2013 and NDIS Rules and Policies
- Disability Inclusion Act 2014
- Ombudsman Act 1974 (amendment Part 3C)
- Aged Care Act 1997
- Aged Care Quality Standards 2019
- Public Health Act 1991 (NSW)

- Health Legislation Further Amendment Act 2004 (NSW) – Schedule 5: Amendment of Public Health Act 1991 (NSW)
- Work Health and Safety Act 2011
- Fair Work Act 2009
- Coroners Act 2009 (NSW)
- Health Records and Information Privacy Act 2002 (NSW)
- Electronic Transmission Act 1999
- Evidence Act 1995
- Australian Standard 4400 - Personal Privacy Protection in Health Care Information Systems
- Office of the NSW Privacy Commissioner – Best Practice Guide – Privacy and People with Decision-Making Disabilities, February 2004
- National Standards for Disability Services, 2014
- The National Disability Insurance Scheme Act (NDIS) 2013
- Australian Government, Commonwealth Home Support Program (CHSP) Guidelines Overview
- NDIS Quality and Safeguarding Framework, 2016
- Australian Government, Department of Health, Home Care Standards, 1 August 2013
- The PRM Group contract requirements
- Information and Privacy Commission New South Wales, IPC Privacy Management Plan, October 2012
- Australian Government, Office of the Australian Information Commissioner, Guide to Information Security – Reasonable Steps to Protect Personal Information, April 2013
- NSW Government, Department of Ageing, Disability and Home Care, Service User Information on privacy and the Minimum Data Set, April 2012

Relevant Lifebridge Documentation

- Pol/GM 1G – Compliance, Quality and Continuous Improvement
- Pol/BM3G – Record and Information Management
- Pol/GM 7 – Information Technology
- Pol/HRM 11 – Flexible Workplace
- SO 13B - Data Breach Response Plan
- SOP 3 – Document Control
- SOP 7 – Recruitment, Selection and Separation
- SOP 55 – Response to Breaches in Privacy
- IH 1 – Staff and Volunteer Handbook