Privacy Policy

Related Legislation and Codes

Privacy Act 1988 (Cth)
Privacy and Personal Information Protection Act 1998 (NSW)
Privacy Amendment Act 2012 (Cth)
Privacy Amendment Act 2017
Australian Privacy Principles (APPs)

1. INTRODUCTION

LLMC is committed to managing personal information in an open and transparent way. LLMC is an un-associated entity under the Uniting Church in Australia NSW.ACT and an accredited Lifeline Centre through Lifeline Australia and is subject to the requirements of the Act. It adheres to the Australian Privacy Principles (APPs) set out in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Federal Privacy Act 1988 (Privacy Act).

2. PURPOSE

The purpose of this policy is to explain how Lifeline mid Coast (LLMC) collects, holds, uses and discloses personal information including sensitive information.

3. APPLICATION

This policy applies to all personal information and sensitive information collected and held by LLMC, and any act done or engaged by LLMC directly related to:

- A current or former employment relationship between LLMC and an individual.
- A current or historical employee record held by LLMC relating to an individual

are exempt from this Policy in accordance with the Act and APPs.

4. DEFINITIONS

Personal Information	Defined under Section 6 of the Privacy Act: "*personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:* *whether the information or opinion is true or not; and* *whether the information or opinion is recorded in a material form or not.*"
Sensitive Information	Information about racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, members of a professional or trade association, membership of a trade union, sexual

	orientation or practices, or criminal record, or health information, genetic information or biometric information.
Notifiable Data Breach	is a data breach that is likely to result in serious harm to any of the individuals to whom the personal information relates. A NDB occurs when personal information held by the Centre is lost or subjected to unauthorised access or disclosure. In such circumstances, LLMC must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as required under the Privacy Amendment (Notifiable Data Breaches) Act 2017.
Employee Record	means a record of confidential personal information relating to employment of a staff member. The employee record comprises information about employment, including: government information requirements, health, terms and conditions of employment, performance, discipline, and resignation. Employee records are exempt from provisions of the Privacy Act.

5. GUIDING PRINCIPLES

Lifeline Mid Coast applies the Australian Privacy Principles (APPs) as set out in Schedule 1 of the Privacy Act 1988 (Cth). The APPs are:

- APP 1 – Open and Transparent Management of Personal Information
  Requires entities to manage personal information in an open and transparent way, including having a clearly expressed and up-to-date privacy policy.
- APP 2 – Anonymity and Pseudonymity
  Individuals must have the option of not identifying themselves, or using a pseudonym, when dealing with an entity (where lawful and practicable).
- APP 3 – Collection of Solicited Personal Information
  Outlines when an entity can collect personal information that is requested, including sensitive information.
- APP 4 – Dealing with Unsolicited Personal Information
  Requires entities to assess unsolicited personal information and, if not legally collectible, destroy or de-identify it as soon as practicable.
- APP 5 – Notification of the Collection of Personal Information
  Entities must notify individuals when collecting personal information, including the purpose and how it will be used or disclosed.
- APP 6 – Use or Disclosure of Personal Information
  Personal information must only be used or disclosed for the purpose it was collected, unless an exception applies.

- APP 7 – Direct Marketing
  Sets rules around using personal information for direct marketing, including providing opt-out options.
- APP 8 – Cross-Border Disclosure of Personal Information
  Entities must ensure that overseas recipients of personal information comply with the APPs or equivalent protections.
- APP 9 – Adoption, Use or Disclosure of Government Related Identifiers
  Restricts the use of government-related identifiers (e.g., Medicare numbers) unless permitted by law.
- APP 10 – Quality of Personal Information
  Entities must take reasonable steps to ensure personal information is accurate, up-to-date, and complete.
- APP 11 – Security of Personal Information
  Requires entities to protect personal information from misuse, interference, loss, and unauthorized access or disclosure.
- APP 12 – Access to Personal Information
  Individuals have the right to access their personal information held by an entity, subject to certain exceptions.
- APP 13 – Correction of Personal Information
  Individuals can request correction of their personal information, and entities must take reasonable steps to correct it.

6. POLICY

Personal Information

Personal Information refers to data that identifies an individual or makes their identity reasonably apparent. This includes sensitive information, such as racial or ethnic origin, political or religious beliefs, trade or professional association membership, sexual preferences, criminal record, health, biometric data, and similar details.

LLMC may collect sensitive information when necessary for its operations and will generally do so with the individual's consent, unless otherwise permitted or required by law. All personal information is collected, used, and disclosed in accordance with LLMC's Privacy Policy and applicable laws. LLMC takes reasonable steps to ensure personal information is securely held.

Collection of Personal Information

LLMC collects personal information only when it is reasonably necessary for its functions and activities. This includes information from staff, volunteers, job applicants,

and other individuals interacting with LLMC for administrative, legislative, business, or research purposes.

Information may be collected directly from individuals through administrative processes, emails, letters, interviews, and other communications. LLMC also generates personal information during its operations, such as recruitment, student placements, service delivery, research applications, and payroll.

Collected information may include:

- Contact details (address, email, phone)
- Date of birth, gender, marital status, family details
- Emergency contact and next of kin
- Identification documents (e.g., passport, driver's licence)
- Bank, tax, and superannuation details
- Employment history, qualifications, and student enrolment data
- Criminal checks, injury records, staying safe plans, and photographs
- Information related to share and option plans

Personal information is stored in both paper, electronic and cloud-based formats.

Information Provided by a third-party and Digital Platforms

As part of its recruitment and operational processes, LLMC may collect personal information from third parties, with the individual's consent where required. This may include:

- Employment history via reference checks
- Visa status to confirm eligibility to work in Australia
- Educational qualifications from academic institutions
- Interview records and results of pre-employment assessments (e.g., aptitude or psychometric tests)
- Medical or allied health assessments to determine capacity to perform role requirements
- Criminal history checks and Working With Children Checks

LLMC may also access publicly available information from networking sites such as LinkedIn or SEEK to support recruitment and engagement activities.

While LLMC does not use cookies to collect data via its website, it may store information about user interactions with its digital platforms to improve services and tailor content. This may include creating digital profiles based on usage patterns.

LLMC's website may contain links to external websites. LLMC is not responsible for the privacy practices of these third-party sites, which are not governed by LLMC's Privacy Policy.

Notification of Collection

When collecting personal information, LLMC will inform individuals of:

- The purpose of collection and its intended use
- Whether the collection is required or authorised by law
- The consequences of not providing the information
- Their rights to access and correct personal information

If personal information is collected without the individual's awareness, LLMC will take steps to notify them.

Information Collected during Employment

Lifeline Mid Coast may also collect information about an individual and their work over the course of their employment with the Company, (or for contractors during the performance of a contract with the Company).

Such information may include:

- details of any contract of employment (or contract for services) including start and end dates, department, role and location, reporting lines, title (including details of previous titles), working days and hours, details of promotions, details of bonuses, remuneration and salary (including details of previous remuneration), benefits and entitlements
- any information relating to disciplinary or grievance investigations and proceedings, including any warnings and related correspondence
- information relating to performance and behaviour at work, including appraisals, ratings, performance reviews, objectives, goals, and performance improvement plans
- details of attendance at work and absences, including annual and personal leave training records including training needs
- details of any expenses claimed; and
- details of the use of Lifeline Mid Coast property and equipment (including computers, swipe cards and telephone systems), emails and software.

Lifeline Mid Coast may also collect other personal information if required or authorised to do so by law.

Use and Disclosure of Personal Information

LLMC collects, holds, uses, and discloses personal information to support its core functions and activities. These purposes include, but are not limited to:

- Business Operations: Conducting and improving LLMC's services and operations, including strategic planning and commercial application of intellectual property and professional expertise.
- Administration: Managing payroll, volunteer coordination, travel bookings, expense reimbursements, and other work-related administrative tasks.

- Recruitment and Employment: Facilitating recruitment, onboarding, appraisals, disciplinary actions, contract management, and termination processes.
- Legal and Compliance: Meeting legislative and regulatory obligations, including government reporting, visa checks, tax and superannuation contributions, and workplace health and safety monitoring.
- Education and Training: Enrolling, teaching, and assessing students and volunteers.
- Research: Conducting and supporting research activities relevant to LLMC's services.
- Stakeholder Engagement: Maintaining contact with stakeholders, engaging with the community, and supporting fundraising initiatives.
- Risk and Incident Management: Handling complaints, injuries, incidents, and insurance matters.
- Security and Access: Ensuring the safety and security of LLMC's buildings, confidential information, and property.
- Professional Services: Engaging legal, HR, industrial relations, accounting, and insurance services as needed.
- Compliance and Investigations: Responding to claims, complaints, investigations, and legal proceedings, including fraud prevention and litigation defence.
- Marketing and Communications: Using personal information (e.g., name, image, job title, work contact details) for legitimate business purposes such as website content, promotional materials, and public communications. In some cases, LLMC may continue to use certain personal information (e.g., staff photos) in marketing materials even after employment ends, always in a reasonable and respectful manner.
- Technology Service Providers: including, internet service providers, cloud hosting service providers, software suppliers, maintenance and support service providers, and security services on a confidential basis so that they can provide services to Lifeline Mid Coast
- To Third Parties: as allowed by law or with your consent

LLMC will only use personal information in accordance with applicable laws and with the individual's consent where required. If you have concerns about how your personal information is used, LLMC encourages you to raise them, and any concerns will be considered thoughtfully.

<u>Use of Personal Information on Lifeline Mid Coast's Website</u>

Lifeline Mid Coast may use your personal information (for example, your name, image, job title and work contact details) on its website or in other publicly available resources where this is necessary for legitimate business purposes.

Lifeline Mid Coast may also use this personal information for other marketing purposes, such as for displaying photos of staff on its website and in other marketing materials. In some circumstances it will be necessary to continue to use certain personal information (such as photos of you) on Lifeline Mid Coast's website or in other marketing materials even after your employment has come to an end.

Lifeline Mid Coast will always only use such personal information in a reasonable manner, considering your position and the nature of your role. If you have any concerns about such use of your personal information, you should discuss this with your manager. Lifeline Mid Coast will consider any such points raised.

Disclosure of Personal Information to Third Parties

LLMC may disclose personal information to third parties when necessary to support its operations, comply with legal obligations, or with the individual's consent.

These disclosures may occur for purposes including:

- Delivering services and fulfilling contractual obligations
- Meeting reporting requirements to government agencies such as the ATO, Fair Work Ombudsman, and WorkCover
- Supporting research initiatives aimed at improving LLMC's services
- Promoting LLMC's activities and community engagement
- Facilitating recruitment, payroll, travel arrangements, and other administrative functions
- Engaging professional services such as legal, HR, accounting, insurance, and industrial relations
- Managing superannuation contributions and employee benefits
- Ensuring building and information security
- Complying with applicable laws or court orders
- Otherwise with the individual's explicit consent

LLMC may also disclose personal information to technology service providers (e.g., cloud hosting, software, and security services), banks, travel agents, and other third-party providers. In all cases, LLMC ensures that these third parties are bound by privacy obligations equivalent to those imposed on LLMC under the Privacy Act 1988 (Cth) and the Privacy and Personal Information Protection Act 1998 (NSW).

Where personal information is disclosed, LLMC takes reasonable steps to ensure that the third party handles the information securely and only for the intended purpose, in accordance with Australian privacy laws.

Accuracy and Storage of Personal Information

LLMC is committed to maintaining accurate, up-to-date, and secure records of all personal information it holds, in accordance with the Privacy and Personal Information Protection Act 1998 (NSW) and APP 13 of the Privacy Act 1988 (Cth).

Individuals are encouraged to ensure that any personal information they provide to LLMC is accurate and current. If your personal details change or you believe LLMC holds incorrect or outdated information, you have the right to request a correction. LLMC will take reasonable steps to correct the information to ensure it is accurate, complete, relevant, and not misleading.

Responsibilities for Handling Personal Information

To ensure personal information is handled appropriately and securely, individuals must:

- Access personal data only when necessary for the proper performance of their role.
- Share personal data only when required for their role.
- Keep personal data secure and protected at all times.
- Regularly review and update personal data as needed.
- Avoid making unnecessary copies of personal data and securely dispose of any copies.
- Use strong passwords to protect documents containing personal data.
- Lock unattended computer screens and devices.
- Never leave computers, devices, files, paperwork, or other items containing personal data in a way that risks unauthorized access or theft.
- Encrypt highly sensitive personal data before transferring it electronically to authorized external contacts. If unsure how to do this, consult your manager or the IT department.
- Consider anonymising data or using separate keys/codes to prevent identification of data subjects.
- Avoid saving personal data to personal computers or devices.
- Refrain from taking personal data off LLMC premises unless necessary for your role.
- Shred or securely dispose of personal data when no longer needed.
- Seek assistance from your manager if you are unsure about any aspect of data protection or believe improvements can be made.
- Immediately report any loss, unauthorized access, security risk, or other issues related to personal information to your manager.

Access to Personal Information

Under the Privacy Act 1988 (Cth), individuals have the right to access personal information that LLMC holds about them, subject to certain exemptions and legal requirements.

Employee Records Exemption

Personal information held by LLMC about current or former employees is generally exempt from the Australian Privacy Principles (APPs) under the employee records exemption. This exemption applies only when the handling of the information is directly related to the employment relationship and involves an employee record as defined under the Act.

Examples include:

- Employment terms and conditions
- Performance and conduct records
- Leave entitlements
- Emergency contact details
- Taxation, banking, and superannuation information

However, this exemption does not apply to:

- Prospective employees or job applicants who were not hired
- Acts or practices unrelated to the employment relationship (e.g., using employee data for marketing purposes)

Access Requests

Individuals who are not covered by the employee records exemption, such as job applicants or contractors, may request access to their personal information by contacting LLMC. LLMC may refuse access or delete information were permitted or required by law.

Unsolicited Personal Information

Unsolicited personal information refers to personal data received by LLMC that was not actively requested or sought. When LLMC receives such information, it will:

- Assess the information to determine whether it could have been lawfully collected.
- If the information has been lawfully collected it will treat it in accordance with the Australian Privacy Principles, which cover notification, use, disclosure, data quality, security, access, and correction.
- If the information could not have been lawfully collected, and it is not part of a Commonwealth record, LLMC will, where lawful and reasonable, destroy or de-identify the information as soon as practicable.

This approach ensures that even unsolicited personal information is afforded appropriate privacy protection.

Destruction of Personal Information

In accordance with Australian Privacy Principle (APP) 11 under the Privacy Act 1988 (Cth), LLMC is committed to ensuring the security of personal information throughout its lifecycle, including its lawful destruction or de-identification when no longer needed.

When LLMC determines that personal information is no longer required for any purpose permitted under the APPs, and is not subject to legal retention requirements or part of a Commonwealth record, it will take reasonable steps to either:

- Destroy the personal information securely, or
- De-identify the information so that it can no longer be linked to an identifiable individual.

LLMC will ensure that destruction or de-identification occurs as soon as practicable after the information is no longer needed, and only where it is lawful and reasonable to do so. This approach helps LLMC minimise the risk of data breaches, comply with privacy obligations, and uphold the trust of individuals whose data it manages.

Raising a Concern or Complaint About Personal Information

If you have concerns about how your personal information, or someone else's, has been handled, you are encouraged to raise the issue promptly.

Reporting options:

- Employees should first discuss their concerns with their manager.
- Other individuals, such as job applicants or contractors, should contact LLMC using the details provided in the Privacy Policy or Customer Complaints, Compliment & Feedback Policy.

LLMC may request that concerns or complaints be submitted in writing to ensure clarity and proper documentation. LLMC will aim to respond within 21 calendar days of receiving the complaint.

Complaints About Breaches of the APPs

Any individual may lodge a complaint if they believe LLMC has breached one or more of the Australian Privacy Principles. These complaints should be made in accordance with LLMC's:

- Workers Grievance Policy, and
- Customer Complaints, Compliments & Feedback Policy

LLMC will assess the complaint and take appropriate steps to investigate and resolve the issue. This may include:

- Reviewing the circumstances of the alleged breach
- Consulting relevant internal stakeholders
- Providing a written response outlining the outcome and any remedial actions

Remaining anonymous or using a pseudonym

LLMC understands that anonymity is an important aspect of privacy and that in some circumstances some people may prefer to use a pseudonym when dealing with LLMC. People have the right to remain anonymous or to use a pseudonym when dealing with LLMC. However, for a significant proportion of its activities (matters relating to employment responsibilities, WHS, enrolment, teaching and assessment) it is impracticable for LLMC to deal with individuals who have not identified themselves or who have used a pseudonym.

Escalation to the Office of the Australian Information Commissioner (OAIC)

If you are not satisfied with LLMC's response, you may escalate the matter to the Office of the Australian Information Commissioner (OAIC). Under Section 36 of the Privacy Act, the OAIC can investigate complaints about acts or practices that may interfere with privacy, including breaches of the APPs. Complaints to the OAIC can be made directly by the individual or through an authorised representative. The OAIC may require supporting documentation and identity verification.

How will LLMC manage an actual or suspected data breach

LLMC will deal with actual or suspected data breach in accordance with the Privacy Data Breach and Response Plan.

7. AUTHORISATION

Authorised by C.Vaara, CEO, on behalf of, UCA Lifeline Mid Coast.