



Privacy Policy

Related Documents

Document	Name
Policy	Privacy Act 1988 Privacy Amendment Act 2012 (Cth) Privacy Amendment Act 2017 Information Management Policy Records & Documentation Policy Employee Records Privacy Policy
Procedures, Manuals, etc.	Code of Conduct Access to Correction of Personal Information Procedure Privacy Data Breach Procedure & Response Plan Privacy Inquiries & Complaints Procedure

Document History

Version	Policy Owner	Reviewer/s	Review Date	Board Approved Date
1	CEO	CEO & Management	Jan 2019	Jun 2019
2	CEO	CEO, Management & Staff,	Jan 2021	Feb 2021

3.11 Privacy Policy

3.11.1 Policy Statement

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).

3.11.2 Privacy purpose

This policy sets out how LLMC collects, holds, uses and discloses personal information including sensitive information.

3.11.3 Application of this policy

Subject to clause 2.3.1, this policy applies to all personal information and sensitive information collected and held by LLMC.

2.3.1 Despite clause 2.3, any act done or practice engaged by LLMC directly related to:

- A current or former employment relationship between LLMC and an individual, and
- 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.

2.3.2 Employee records are governed by the provision of LLMC Employee Records Policy.

3.11.4 Privacy Principles

3.11.5 Personal information collected and held by LLMC

LLMC collects personal information for the purposes of LLMC's functions and activities. It collects personal information about staff, volunteers and other individuals who have dealings with the organisation for administrative needs, to conduct business, for legislative compliance or for research purposes.

The information may include residence and contact details, date of birth, details of next of kin, identifying information, including photographs, records of injuries, criminal checks, student enrolment information, qualifications, financial information, staying safe plans and information collected for or concerning research connected to LLMC services.

Some of the information LLMC collects and holds is sensitive information. LLMC only collects sensitive information where it is necessary for the purposes for which it is being collected and with the individuals consent unless the collection is required or authorised by law.

3.11.6 How LLMC collects and holds personal information

LLMC collects and holds information from a number of sources. Where reasonably possible, LLMC will only collect information from the individual to whom it relates. Frequently this will be collected through LLMC administrative processes but it may also be collected from email, letters, interviews and other forms of communication. LLMC also holds personal information about individuals that it generates in the course of its operational activities such as recruitment information, student placement information, service delivery information, research grant applications and payroll.

Personal information is held in paper and electronic form, including data bases.

Although LLMC has a website, we do not use “cookies” to collect and/or use data obtained through the website. However, to improve LLMC services and to assist visitors to the website or other digital platforms such as Facebook, LLMC may store information about uses our website or digital platforms to create a digital profile and provide them with information specific to them.

The LLMC website may contain links to other websites. LLMC cannot control the privacy controls of third party websites. Third party websites are not subject to LLMC’s Privacy Policy or Procedure.

3.11.7 Notification of collection of personal information

When LLMC collects personal information, it will advise the individual why it is collecting that information and how it uses it, whether the collection of the information is required or authorised by law and the consequences for the individual if the personal information is not collected. It will also provide information about LLMC’s Privacy Policy and about the rights of individuals to access and correct personal information. If LLMC collects personal information in circumstances where the individual may not be aware of the collection it will seek to advise the individual of the collection.

3.11.8 The purposes for which LLMC collects, holds, uses and discloses personal information

LLMC collects and uses personal information for a variety of different purposes relating to its functions and activities including:

- Conducting business and improving the way in which it conducts its business
- Administrative tasks including; process payroll and volunteer needs
- Government reporting
- Enrolling, teaching and assessing its students/volunteers
- Undertaking recruitment activities
- Undertaking research
- Maintaining contact with stakeholders
- Community engagement
- Fundraising
- Handling complaints
- Handling injuries/incidents
- Community engagement
- Commercial application of its intellectual property and professional expertise
- Purposes directly related to the above

3.11.9 Use or disclosure for secondary purposes

LLMC does not use or disclose personal information for purposes other than the purpose for which it was collected (the primary purpose) unless:

- The individual has given consent for secondary use or disclosure, or
- The secondary use or disclosure is related to the primary purpose (in the case that is not sensitive information) or is directly related to the primary purpose (in the case of sensitive information), or
- It is otherwise required or authorised by or under an Australian law or a court/tribunal order, or
- A permitted general situation exists (as described in clause 26 Glossary of Terms), or
- LLMC reasonably believes that it is necessary for one or more reinforcement related activities conducted by, or on behalf of an enforcement body.

In ordinary circumstances, any disclosure of personal information for a secondary purpose must be approved by the Office Manager.

3.11.10 Security

LLMC updates both physical and digital security systems to protect personal information. Systems are in place to protect from loss, inappropriate access, mis-use, alteration of electronic records.

See B) 8 Human Resource Records for procedures.

3.11.12 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.

3.11.13 Unsolicited personal information

When LLMC receives unsolicited personal information, it will assess whether it is personal information that it could legally collect. If it is, it will treat it according to the APPs. If it is not, it will if lawful to do so, destroy or de-identify it as soon as practicable.

3.11.14 Direct marketing

LLMC will only use personal information for direct marketing with the individual's consent or when authorised by law.

3.11.15 Destruction of information that does not need to be retained

When LLMC no longer needs to retain personal information, and is lawfully able to do so, it will destroy or de-identify that information.

3.11.16 How an individual may access personal information

Subject to the Privacy Act, anyone has the right to access personal information that LLMC holds about them. Access to personal information is governed by the procedures set out in Section 4: Administration.

3.11.17 How an individual may seek the correction of personal information

Anyone has the right under the Act to request correction to any personal information that LLMC holds about them if they think the information is inaccurate, out of date, incomplete, irrelevant or misleading. Correction of personal information is governed by the procedures set out in Section 4: Administration.

3.11.18 How an individual may complain about a breach of the Australian Privacy Principles (APPs) by LLMC

Anyone may complain about a breach of an APP by LLMC. Complaints should be made in accordance with the LLMC's Feedback and Complaints Handling Policy,

3.11.19 How LLMC will deal with complaints about breaches of the Australian Privacy Principles (APPs)

LLMC will deal with complaints about breaches of the APPs in accordance with the Inquiries and Complaints Procedures.

3.11.20 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.

3.11.21 Disclosure of personal information to third parties

LLMC may disclose information to third parties to:

- Provide services
- To government bodies when required by law
- For the purposes of research to improve its operations and services
- Promote its activities
- If permitted by law, or
- Otherwise with the consent of the individual

Where LLMC discloses personal information to third parties it will require restrictions on the collection and use of personal information equivalent to those required of LLMC by the Privacy Act 1988.

3.11.22 Roles & Responsibilities

The LLMC Board and CEO are the approval authority of this policy

The Governing Authority of this policy is the LLMC Board.

The Responsible Officer and Privacy Officer is the CEO of LLMC

The Privacy Coordinator is the Office Manager of LLMC

3.11.23 Policy Review

LLMC will review this policy and the procedures regularly. It may amend the policy and procedures from time to time to ensure their currency with respect to relevant legislation and LLMC policy and procedures and to improve the general effectiveness and operation of the policy and procedures.

In line with the LLMC Development and Review Policy and Procedures, this policy is scheduled for review every 3 years or sooner in the event that the Approval Authority or Governing Authority determine that a review is warranted. The policy and procedure will be initially reviewed one year following effective date.

3.11.24 Further Assistance

Access to this policy in alternative formats (e.g. hard copy) is available through the Privacy Coordinator (Office Manager) whose contact details are listed under contact details at the end of the policy.

3.11.25 Contact Details

Contact for all matters related to privacy, including:

- General inquiries
- Accessing personal information held about you
- Request to correct personal information held about you
- Complaints about breaches of privacy

Should be directed as follows:

Office Manager (Privacy Coordinator)

Email: finance@lifelinemidcoast.org.au

Phone: (02) 6581-2800

Address: Lifeline Mid Coast office: 5 Sherwood Rd, Port Macquarie, NSW 2444

Post: P.O. Box 5030, Port Macquarie, NSW 2444

3.11.26 Glossary of Terms

Access Procedure means the Access to and Correction of Personal Information Procedure stated under this policy.

Act means the Privacy Act 1988 (Cth)

Australian Policy Principles (APPs) means the 13 APPs set out in Schedule 1 of the Act.

Data breach means the loss, unauthorised access to, or disclosure of personal information.

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.

Inquiries and Complaints Procedure means the Privacy Inquiries and Complaints Procedure stated under this policy.

Loss means accidental or inadvertent loss of personal information likely to result in unauthorised access or disclosure. For example, an employee leaves a copy of a document or a device on public transport. If data can be deleted remotely or is encrypted it will not constitute a Notifiable Data Breach (NDB).

Notifiable Data Breach (NDB) 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.

Permitted general situation has the same meaning as provided for in section 16A of the Act and referred to in APP 6 2(C). The permitted general situations are: lessening or prevention a serious threat to life, health or safety of any individual, or to public health, or safety; taking appropriate action in relation to suspected unlawful activity or serious misconduct; locating a person reported missing; asserting a legal or equitable claim; conducting an alternative dispute resolution process.

Personal information means information or an opinion in any form about an identifiable individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not.

Privacy Coordinator means the person appointed by LLMC from time-to-time to manage and coordinate LLMC's compliance with the policy and procedures at the direction of the CEO (Privacy Officer).

Privacy Officer means the person appointed by LLMC from time-to-time to manage all inquiries and complaints arising under this policy. The Privacy Officer (CEO) may delegate the management of any or all of the inquiries and complaints arising under this policy to the Privacy Coordinator.

Sensitive information means 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.

Serious harm is determined with regard to the following list of relevant matters as provided for in section 26WG of the Privacy Amendment (Notifiable Data Breaches) Act 2017: The kind of information:

- The sensitivity of the information.
- Whether the information is protected by one or more security measures.

- If the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome.
- The persons, or kinds of persons, who have obtained, or who could obtain, the information.
- If a security technology or methodology:
 - Was used in relation to the information; and
 - Was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information.
- The likelihood that the persons, or the kinds of persons, who:
 - Have obtained, or who could obtain the information.
 - Have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates.
 - Have obtained, or could obtain information or knowledge required to circumvent the security technology or methodology.
- The nature of the harm.
- Any other relevant matters.

Unauthorised access means personal information accessed by someone who is not permitted to have access. This could include an employee or the organisation, a contractor or external third party (such as hacking).

Unauthorised disclosure means where an organisation releases/makes visible the information outside the organisation in a way not permitted by the Privacy Act.

For example, an employee accidentally publishes a confidential data file containing personal information on the internet.

Web Analytics means the measurement collection, analysis and reporting of web data for the purpose of understanding and optimising web usage.