



Policy Number:	ML 1.5	Date:	23 rd October 2018
		Approved by:	Chief Executive Officer
Version:	1/2018	Scheduled review date:	1 st November 2019

1. Statement of Context and Purpose

- 1.1 Melbourne Legacy (ML) is committed to ethical practices and standards. This includes respecting the privacy of all personal information in its possession.
- 1.2 This policy aims to:
 - (a) outline how ML handles personal, sensitive and health information to comply with applicable privacy legislation;
 - (b) direct employees on the responsible collection and handling of personal information; and
 - (c) support the principle of responsible and transparent handling of personal information.

2. Scope

- 2.1 This policy applies to all employees, contractors, volunteers and other authorised personnel required to perform functions on behalf of ML or on ML's premises.
- 2.2 This policy is not intended to override or form part of the terms of any award, enterprise agreement or contract that applies to an employee, but should be considered a reasonable direction to staff. As such all employees, volunteers, contractors and other authorised personnel are expected to abide by this policy and report any suspected or known breaches of this policy.

3. Related Documents

3.1 External Documents

Relevant Legislation or Authority:

- a) Archives Act 1983
- b) Privacy Act 1988 (Cth)
- c) Privacy and Data Protection Act 2014 (Vic)

3.2 Internal Documents

Policies and Procedures:

- a) Code of Conduct
 - b) Disciplinary Policy
-

4. Definitions

- 4.1 **Access** means the ability to view, obtain or retrieve information in any form to any other person.
- 4.2 **Confidentiality** for the purposes of data security, confidentiality refers to the limiting of official information to authorised persons for approved purposes, commonly understood as the 'need to know'.
- 4.3 **Direct Identifier** means any information that directly identifies a single individual. Direct identifiers may consist of one or more variables that can be used to identify an individual, either by themselves or in combination with other readily available sources of information. Examples may include name, address, email address.
- 4.4 **Disclosure** amounts to making the information accessible or visible to others outside the organisation holding the information.
- 4.5 **Hold** means the information is contained in a document that is in the possession or under the control of ML. This can be solely in the possession or control of ML or another organisation. The location of the document is irrelevant.
- 4.6 **Integrity** for the purposes of data security, integrity refers to the assurance that information is only created, modified or deleted only by intended and authorised means and it is correct and valid.
- 4.7 **Loss** means that the physical whereabouts of information is unknown (including both hard and/or soft copies) and involves the failure to preserve or maintain the information in a known place. Loss does not include the intentional destruction or de-identification of information.
- 4.8 **Misuse** means personal or health information is misused if it's used in a way that contravenes any of the information or principles of this policy, which deal with use and disclosure.
- 4.9 **Modification** means the changing, removing or adding of components to the original information.
- 4.10 **Personal information** is defined in the *Privacy and Data Protection Act 2014* (Vic) and includes any information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can be reasonably ascertained from the information or opinion but does not include information of a kind to which the Health Records Act 2001 applies. Examples include:
 - (a) Name, address, birth date, telephone number, email address;
 - (b) Age, sex, marital status;
 - (c) Employment, educational, financial or criminal history;
 - (d) An image in a photograph or a voice in a recording;
 - (e) Location data, device details, online identifier (in some circumstances)

- 4.11 **Quasi Identifiers** do not of themselves enable the identification of an individual but can be aggregated and linked with other information to identify an individual. Examples include, date of birth, age, gender, postcode and other demographic information.
- 4.12 **Sensitive information** is defined in the *Privacy and Data Protection Act 2014* (Vic) to mean information or an opinion about an individual's:
- (a) Racial or ethnic origin; or
 - (b) Political opinions; or
 - (c) Membership of political associations; or
 - (d) Religious beliefs or associations; or
 - (e) Philosophical beliefs or associations; or
 - (f) Membership of a professional or trade association; or
 - (g) Membership of a trade union; or
 - (h) Sexual orientation or practices; or
 - (i) Criminal record,
- that is also personal information.
- 4.13 **Unauthorised Access, modification or disclosure** means access, modification or disclosure of information that is considered unauthorised where an individual:
- (a) Has no proper authority to access, modify or disclose the information; or
 - (b) Exceeds their authority by acting beyond their power; or
 - (c) Misuses their authority to access, modify or disclose the information.
- 4.14 **Unique Identifier** is defined in the *Privacy and Data Protection Act 2014* (Vic) to mean an identifier (usually a number, such as an employee or payroll number) assigned by an organisation to an individual to uniquely identify that individual for the purposes of the operations of the organisation.
- 4.15 **Worker** is broadly defined, and for the purposes of this policy may mean:
- (a) An employee;
 - (b) A contractor or subcontractor used by ML;
 - (c) An employee of a contractor or subcontractor used by ML;
 - (d) An employee of a labour hire company used by ML;
 - (e) An apprentice or trainee or work experience student employed by or hosted by ML;
 - (f) A student gaining work experience or undertaking a vocational placement with ML;
 - (g) A volunteer or Legatee.

5. Responsibilities

- 5.1 All workers are responsible for being aware of and complying with this policy.
- 5.2 All Legatees, employees, contractors and service providers must handle personal information in accordance with the Privacy Act 1988 (Cth), the principles of this policy and other relevant Melbourne Legacy policy and procedures.

6. Collection of Personal and Sensitive Information

- 6.1 It is necessary for Melbourne Legacy to collect and store personal information in order to deliver certain services and programs. Melbourne Legacy mostly collects personal information directly from the individual concerned. However, in some circumstances, Melbourne Legacy may collect personal information from a third party the individual has

authorised to provide the information or where it is unreasonable or impracticable to collect it from the individual.

- 6.2 Melbourne Legacy may also collect personal information from a government agency, such as the Department of Veterans Affairs (DVA) to obtain service history information, support requests and other pertinent information to administer either support or pension claims.
- 6.3 The types of personal information collected and held by Melbourne Legacy may include:
- a) names, date of birth, occupation, marital status, residential details, details of dependents, date of death
 - b) pension, medical, clinical, advocacy, personal case, social work and rehabilitation files
 - c) financial information, including income and asset details, and
 - d) service history
- 6.4 Where practicable and necessary, Melbourne Legacy will collect personal information directly from the individual with their consent. Where personal information is provided to ML by a person other than the consenting individual, Melbourne Legacy will:
- (a) De-identify or destroy the information if it is not to be retained; or
 - (b) If the information is to remain identified and be retained, provide the person to whom the information relates a copy of the relevant privacy collection statement explaining the purposes of collection, where such a statement has not already been provided.
- 6.5 Sensitive and personal information will only be collected if it is directly related to the primary purpose for which the information will be collected or as required by law or with the individual's specific and informed consent.
- 6.6 The sensitive information collected by Melbourne Legacy relates mostly to:
- a) health or medical information, including mental health and disabilities, and
 - b) age, racial or ethnic origin of an individual, for example for inclusion into statistics or the indigenous veteran database.
- 6.7 In certain circumstances, personal information may be collected by people or organisations acting and providing services on behalf of Melbourne Legacy, such as contracted health, rehabilitation and aged care service providers and medical and health care professionals in the case of partnership or outsourcing. Similarly, personal information may be collected by contractors who provide services to Melbourne Legacy such as contracted Information and Communications Technology (ICT) providers. Records collected or created by contractors under Melbourne Legacy contracts are owned by Melbourne Legacy. Additionally, Melbourne Legacy's obligations under the Privacy Act regarding the collection of personal information are extended to contractors (or subcontractors) under Melbourne Legacy contracts.
- 6.8 In limited circumstances, Melbourne Legacy is authorised to collect Tax File Numbers (TFNs) for administering paperwork for certain payments. There is no obligation to provide a TFN. However, some payments, such as pensions and allowances, cannot be made without the provision of a TFN. Melbourne Legacy's handling of TFNs is governed by the Privacy (Tax File Number) Rule 2015, which can be accessed at: www.comlaw.gov.au.
-

7. Storage and Security

- 7.1 Melbourne Legacy stores all personal information securely and restricts access to Legatees, employees, contractors and service providers who require access to the personal information to perform their duties or assist the individual concerned.

- 7.2 Melbourne Legacy will store personal information in a variety of formats, including on computer and paper media (for example electronic databases and physical files). Melbourne Legacy uses a range of IT and physical security systems to protect the personal information it holds and takes reasonable steps to ensure that information is protected from misuse, interference, loss, unauthorised access, modification and disclosure. Legatees should forward all records to staff for storage so that no records are retained off site.
- 7.3 Melbourne Legacy may contact individuals to determine whether personal information collected should be retained. If Melbourne Legacy no longer requires the personal information, it will take reasonable steps to destroy or de-identify the personal information, unless the information is contained within a Commonwealth record. If the information is contained within a Commonwealth record, the record can only be destroyed or altered in accordance with the Archives Act 1983.
- 7.4 Melbourne Legacy will take reasonable steps to ensure that personal, sensitive and other information is collected, maintained, used or disclosed and is:
- (a) Accurate, complete and up to date;
 - (b) Protected from misuse, loss, unauthorized access, modification or disclosure; and
 - (c) Securely destroyed or permanently de-identified when no longer required.
- 7.5 Physical, technical and appropriate protective data security practices are applied to all personal information held by Melbourne Legacy.
- 7.6 When using contracted service providers, Melbourne Legacy endeavors to ensure contracted service providers are subject to a law, binding scheme or contract that provides similar protection of the personal information as provided for by the privacy principles.
- 7.7 Where there is a change to an existing service, system or process, Melbourne Legacy will conduct a Privacy Impact Assessment to:
- (a) Ensure legal obligations are met to protect the privacy of any personal and sensitive information Melbourne Legacy collect, use, disclose or store;
 - (b) To support good governance and informed decision making in the handling of personal and health information;
 - (c) To ensure appropriate risk mitigation considerations in the handling of personal or sensitive information are considered;
 - (d) To assess whether it is safe and appropriate to proceed to the implementation phase of a new activity/project/process; and
 - (e) To consider the non-legal risks related to the planned change, such as but not limited to, individuals being uncomfortable with the use of their information for particular purposes that Melbourne Legacy should be sensitive to.

8. Access, Use, Modification and Disclosure of Personal and Sensitive Information

8.1 Use and Disclosure

- 8.1.1 Melbourne Legacy generally uses and discloses personal information for the primary purpose for which it was collected. These primary purposes include but are not limited to:
- a) assisting with pension claims, compensation and advocacy
 - b) providing case management
 - c) providing social and emotional support
 - d) facilitating programs, activities and event.

- 8.1.2 When Melbourne Legacy collects personal information about an individual, Melbourne Legacy is required to take reasonable steps to notify the individual of certain matters, including the purposes of collection and other entities (such as government agencies), bodies or persons to which the information is usually disclosed.
- 8.1.3 In certain circumstances, Melbourne Legacy may use or disclose information in its possession for a different purpose (the secondary purpose), such as where the individual has consented or would reasonably expect Melbourne Legacy to use or disclose the information for a secondary purpose, and the secondary purpose is:
- a) related to the primary purpose for which the information was collected (or in the case of sensitive information, directly related to the primary purpose), or
 - b) required or authorised under Australian law or has been ordered by a court or tribunal, or
 - c) reasonably necessary for enforcement related activities.
- 8.1.4 In addition, personal information (including sensitive and/or health information) may be used or disclosed if it is necessary to lessen or prevent:
- (a) A serious threat to an individual's life, health, safety or welfare; or
 - (b) A serious threat to public health, public safety or public welfare.
- 8.1.5 Similarly, personal or sensitive information may be disclosed to law enforcement and government bodies, insurers, employees and contractors, and third parties who provide services to Melbourne Legacy or as required by law.
- 8.2 Access
- 8.2.1 Individuals may access their own personal information which Melbourne Legacy holds about them. Melbourne Legacy cannot provide an individual with the personal information of a partner or family member without consent or other lawful authority, such as to a legal guardian, nominated representative or authorised agent acting on behalf of an individual.
- 8.2.2 There is no cost associated with requesting access to personal information. Melbourne Legacy will respond to most requests for access to personal information within 14 days of the request being received. In some circumstances, a request for personal information can be refused, including where the information is subject to legal professional privilege. If Melbourne Legacy decides to refuse access to the information a written notice of the reasons for refusal will be provided.
- 8.2.3 Although the information of a deceased individual is not regulated by the Privacy Act 1988, Melbourne Legacy will continue to respect the sensitivities of family members when using or disclosing such information.
- 8.3 Modification
- 8.3.1 Under of the Privacy Act 1988, individuals may make a request to Melbourne Legacy to amend personal information that is out-of-date, incomplete, irrelevant or misleading. Melbourne Legacy will respond to most requests for correction of personal information within 14 days of the request being received. There is no cost associated with requesting correction of personal information.
- 8.3.2 In some circumstances, a request to correct personal information can be refused.

9. Privacy Incidents and Complaints

9.1 Privacy Incidents

- 9.1.1 If an individual becomes aware of a privacy incident, the incident should be reported directly to Melbourne Legacy for advice, assessment and possible investigation and response.
- 9.1.2 A privacy incident means a suspected or potential breach of this policy, and may include:
- (a) The use or disclosure of personal or health information for a purpose that is not authorised by the individual or by law; or
 - (b) The loss, misuse, unauthorised access, modification or disclosure of personal or health information.
- 9.1.3 Where appropriate, Melbourne Legacy will investigate the privacy incident and provide a report on the outcome of the investigation and the actions recommended to address the incident.
- 9.2 Privacy Complaints
- 9.2.1 Complaints forwarded to Melbourne Legacy should include:
- a) a brief description of the privacy concern;
 - b) any action the complainant or Melbourne Legacy has taken to fix the problem; and
 - c) copies of any relevant documents.
- 9.2.2 Melbourne Legacy will record complaints about potential privacy breaches and onforward the detail of the complaint to Melbourne Legacy's law firm for investigation and reporting purposes.
- 9.2.3 Melbourne Legacy aims to acknowledge complaints received by telephone and email within two working days and to resolve the issue within 28 days. For complaints received by mail, Melbourne Legacy aims to provide acknowledgement within fourteen working days and to resolve the issue within 28 days. If the matter is complex, it may take longer. In such cases, Melbourne Legacy will ensure the complainant is given the contact details of the person assigned to managing their complaint and will keep them informed of progress and an expected resolution date.
- 9.2.4 Where a complainant is dissatisfied with the way Melbourne Legacy handles their privacy related complaint, they may contact the Office of the Australian Information Commissioner on 1300 363 992 or via the internet at <http://www.oaic.gov.au>
-

10. Consequences of a Breach of this Policy

- 10.1 ML emphasises the need to comply with the requirements of this policy. Breaches of this policy and its procedures may result in suspension of access to ML's information resources.
- 10.2 Any employee found to be in breach of the requirements of this policy may be subject to disciplinary action, up to and including termination of employment. Employees should refer to the Performance Management, Misconduct and Disciplinary Action Policy and Procedure.
- 10.3 Similarly, a Legatee or volunteer found to be in breach of the requirements of this policy may be subject to disciplinary action in accordance with ML's Legatee Code of Conduct.
-

11. Policy Review

- 11.1 ML may make changes to this Policy at any time and will inform Legatees, volunteers and staff accordingly.
-

12. Authorisation

Approved by Melbourne Legacy Chief Executive Officer:

Justin Elwin

Date: 23 / 10 / 2018

Ratified by:

Melbourne Legacy Board of Management

Date: 23 / 10 / 2018
