

**Category:** Governance and Management

**Version:** 9

**Document Type:** Policy

**Document Status:** Published

**Approved On:** 10 August, 2023

**Audience:** Staff, Students, Research, Academic

**Effective Date:** 28 November, 2023

**Review due by:** 11 March, 2021

**Policy Approver:** Vice-President Administration & Finance And Chief Operating Officer

**Policy Steward:** University Secretary

**Supporting Process:**

Governance and Management Processes

## Privacy Policy (MPF1104)

### 1. Objective

1.1. The objectives of this policy are to:

- a) identify the University's obligations for handling personal information of past and present University staff, students, prospective students and other individuals associated with the University;
- b) encourage all University staff to take a proactive privacy approach; and
- c) identify the University's obligations for responding to complaints about potential privacy breaches.

### 2. Scope

2.1. This policy applies to all personal and health information (including sensitive information) collected by the University, including that of staff and students and other individuals associated with the University.

### 3. Authority

3.1. This policy is made under the University of Melbourne Act 2009 (Vic) and the Vice-Chancellor Regulation. It supports compliance with the:

- a) Privacy and Data Protection Act 2014 (Vic);
- b) Health Records Act 2001 (Vic);
- c) Public Records Act 1973 (Vic);
- d) Privacy Act 1988 (Cth) in circumstances where the University agrees to be bound contractually under the Commonwealth privacy legislation, or where it is subject to specific provisions, such as the Notifiable Data Breaches (NDB) scheme which applies to the University as a Tax File Number Recipient; and
- e) European Union General Data Protection Regulation (GDPR) in circumstances where the GDPR applies to the University's activities involving individuals or entities located in the European Union (EU), or where the University enters into a binding contract requiring it to abide by the provisions of the GDPR.

### 4. Policy

4.1. Proactive privacy – The University is proactive in its approach to privacy protection by anticipating and preventing invasive events before they occur.

4.2. Privacy by design – The University embeds privacy considerations into the design and architecture of information technology systems and business processes.

4.3. The University collects, uses, discloses and manages personal information as University records in accordance with the Information Privacy Principles (IPPs) in the Privacy and Data Protection Act 2014 (Vic).

4.4. In circumstances where the Privacy Act 1988 (Cth) applies the University will:

- a) comply with Australian Privacy Principles (APPs) that have the same intent as the IPPs in the Victorian legislation; and
- b) meet its obligations under the NDB.

4.5. In circumstances where the GDPR applies to the University's activities, the University will act in accordance with its requirements.

4.6. The University collects health information of its staff, students and other individuals, in accordance with the Health Privacy Principles (HPPs) in the Health Records Act 2001 (Vic).

## 5. Procedural principles

5.1. The University's Privacy and Data Protection Officer is responsible for responding to all complaints of potential privacy or personal data protection breaches.

5.2. Privacy impact assessments (PIAs) must be undertaken throughout the development and implementation of any project that collects, handles, processes or discloses personal information, or when making changes to existing systems or activities.

5.3. General privacy statements must be available on the University's privacy website .

5.4. Privacy collection notices specific to particular projects or activities must be provided at the point of collection of any personal information from individuals.

5.5. Both the general website privacy statements and specific privacy collection notices must include the following information:

- a) the main functions of the University (or relevant area/s of the University) and the types of personal information collected to fulfil these;
- b) the name and contact details of the appropriate University representative in relation to those functions;
- c) the purposes of collection of the information;
- d) how personal information is used and to whom it is routinely disclosed;
- e) whether collection of personal information is optional or compulsory under applicable legislation;
- f) how the information is stored securely, how access is properly managed, and the retention periods for the information;
- g) details of any transfer or storage of the information outside Victoria and how privacy is protected in such circumstances;
- h) how individuals can request access to, or correction of, their personal information, or exercise GDPR rights where applicable; and
- i) the name and contact details of the University's Privacy and Data Protection Officer (DPO).

## 6. Roles and responsibilities

<i>Role/Decision/Action</i>	<i>Responsibility</i>	<i>Conditions and limitations</i>
-----------------------------	-----------------------	-----------------------------------

The Privacy and Data Protection Officer must control and maintain the Privacy Policy	University Secretary	
The Privacy and Data Protection Officer must administer this policy, including monitoring compliance, informing and assisting staff on privacy issues and responding to complaints concerning potential privacy breaches	University Secretary	
The Privacy and Data Protection Officer is the contact point for the purposes of the GDPR	University Secretary	

## 7. Definitions

**Australian Privacy Principles** means the set of 13 principles in the [Privacy Act 1988 \(Cth\)](#) governing the collection, quality, use, disclosure, management and transfer of personal information.

**General Data Protection Regulation** means the legal framework governing the collection and processing of personal information of individuals located in the European Union (EU). The GDPR has extraterritorial reach and applies to entities outside the EU which do business with individuals located in the EU.

**Health information** has the meaning given to it in section 3 of the [Health Records Act 2001 \(Vic\)](#).

**Health Privacy Principles** means the set of 11 principles in the [Health Records Act 2001 \(Vic\)](#) governing the collection, management, use, disclosure and transfer of health information by organisations such as the University.

**Information Privacy Principles** means the set of 10 principles in the [Privacy and Data Protection Act 2014 \(Vic\)](#) governing the collection, use, disclosure, management and transfer of personal information by organisations such as the University.

**Notifiable Data Breach scheme (NDB)** means eligible data breaches that fall under the Commonwealth mandatory reporting scheme. As a Tax File Number Recipient, this applies to the University in relation to any unauthorised access to, or unauthorised disclosure of, tax file number data.

**Personal information** has the meaning given to it in section 3 of *the* [Privacy and Data Protection Act 2014 \(Vic\)](#)

**Personal data** has the meaning given to it in Article 4 of the European Union General Data Protection Regulation.

**Privacy by design** means a methodology to build privacy and data protection into the design and architecture of information systems, business processes and networked infrastructure.

**Privacy impact assessment** means a risk analysis tool to identify and mitigate privacy and data protection risks, and to identify and evaluate privacy solutions.

**Proactive privacy** means focusing on prevention rather than remediation.

**Sensitive information** has the meaning given to it in schedule 1 of the [Privacy and Data Protection Act 2014 \(Vic\)](#).

**University record** means recorded information, in any format (eg electronic, paper, image) created or received by staff of the University in the course of conducting their University duties.

## POLICY APPROVER

## **POLICY STEWARD**

University Secretary

## **REVIEW**

This policy is to be reviewed by 11 March 2021.

## **VERSION HISTORY**

<b>Version</b>	<b>Approved By</b>	<b>Approval Date</b>	<b>Effective Date</b>	<b>Sections Modified</b>
1	Council	8 October 2012	8 October 2012	New version arising from the Policy Simplification Project. Loaded into MPL as Version 1.
2	University Secretary	23 March 2016	23 March 2016	Update legislation reference to the Privacy and Data Protection Act 2014 (Vic).
3	Vice-Chancellor	11 March 2016	21 July 2016	New version arising from the Policy Consolidation Project. This policy and its supporting processes replace the Privacy Policy and the Privacy Procedure MPF1105.
4	University Secretary	18 August 2016	18 August 2016	Add hyperlink to Privacy Impact Assessment in section 5.2.
5	University Secretary	13 September 2016	5 October 2016	Update hyperlink to Privacy Impact Assessment in section 5.2. Correct error identified in version history table.

6	Vice-Chancellor	7 March 2019	19 August 2019	Changed Policy Approver to Vice-President (Strategy & Culture) (previously Vice-Chancellor).
7	Vice-President (Strategy & Culture)	16 August 2019	19 August 2019	Incorporated new provisions relating to the European Union General Data Protection Regulation and Commonwealth Notifiable Data Breaches scheme. Amended Policy Steward title. Editorial amendments to correct minor errors or align with the University's policy style guide.
8	Policy Officer	30 November 2022	30 November 2022	Formatting changes.
9	Vice-President Administration & Finance and Chief Operating Officer	10 August 2023	28 November 2023	Policy Approver updated to reflect retirement of Vice-President (Strategy & Culture) role.