Privacy Policy (MPF1104)

1. Objective

1.1. The objectives of this policy are to:

a) outline the University of Melbourne ("University") approach to privacy management;

b) define the University's privacy governance model;

c) identify the University's obligations when processing personal information; and

d) embed a culture of privacy awareness and good practice throughout the University.

2. Scope

2.1. The University collects and processes personal information that is necessary for delivering one or more of its functions or activities, including but not limited to teaching, learning and research, as defined in the objects of our enabling legislation.

2.2. This policy applies to all personal, sensitive and health information (together "personal information") collected or held by the University, including information about employees, students and any other individuals associated with the University.

2.3. This policy applies to all employees, including non-academic departments and entities owned by the University.

2.4. This policy also applies to individuals or organisations (and their officers and employees) who are contractually obliged to comply with this policy.

2.5. University's controlled entities may choose to adopt this policy in accordance with section 5.3 of the Controlled Entities Policy (MPF1376).

2.6. Entities not owned or controlled by the University, such as affiliated organisations or partnerships, are not automatically covered by this policy. However, they may have separate agreements in place that address specific aspects of it.

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 applicable privacy and data protection laws, including:

a) The *Privacy and Data Protection Act 2014* (Vic) and the Victorian Information Privacy Principles (IPPs);

b) The *Health Records Act 2001* (Vic) and the Health Information Principles (HPPs);

c) The Commonwealth *Privacy Act 1988* for certain regulated information, including Tax File Numbers, or when the University contractually agrees to comply with this Act; and

d) International privacy and data protection law (see definition), to the extent that these apply to our activities.

4. Policy

4.1. The University respects the privacy of anyone it interacts with and is committed to the compliant, responsible and fair management of personal information upheld by a culture of good privacy governance and practices that our community can rely on.

4.2. Information privacy is managed in accordance with the University's Privacy Management Framework (login required).

4.3. The University's approach to privacy management is upheld by the following core principles:

a) **Privacy by design**: We proactively embed privacy considerations and strategies into the design of our systems, processes, and practices.

b) **Transparency and Fairness**: We provide clear and transparent information about the University's main functions, the types of personal information we collect, and how we use, share and manage that information, including when using emerging technologies, through accessible University Privacy Statements. This supports individuals in making informed decisions and helps ensure our practices are fair, reasonable and aligned with community expectations.

c) **Automated decision-making and Profiling:** We ensure that any use of Automated Decision-Making or profiling respects individuals' privacy, is transparent, and upholds principles of fairness and accountability.

d) **Security**: We take reasonable steps to ensure that personal information is protected throughout the information lifecycle.

e) **Compliance**: We manage personal information in compliance with applicable domestic and international privacy and data protection laws.

f) **Data Minimisation**: We collect, manage, and retain the minimum amount of personal information that we need, in an ethical and fair manner that respects individual interests.

g) **Community expectations:** We manage personal information according to best practices and regulatory requirements.

4.4. Where inconsistencies might exist between applicable privacy and data protection laws, the University will be guided by best practice privacy management and will seek to meet the most comprehensive legal obligations, ensuring the highest standard of privacy protection. All employees must seek guidance from the Privacy and Data Protection team to ensure this standard is met.

5. Procedural principles

5.1. The University's designated Privacy and Data Protection Officer ("PDPO") oversees compliance with privacy and data protection laws, policies and processes, assessments, and audits.

5.2. The University's Privacy and Data Protection team supports the PDPO by operationalising the University's privacy management program, including providing guidance on privacy obligations and responsibilities.

5.3. All employees are responsible for the compliant management of personal information throughout the information lifecycle, which includes:

a) **Collection**: Collecting the minimum amount of information required to effectively fulfil a necessary function and doing so by lawful and fair means. Providing individuals with an adequate Privacy Collection Notice at or before the time of collection, clearly explaining:

i. why we are collecting their personal information;

ii. how it will be processed; and

iii. how individuals can access or correct their information.

b) **Consent**: Where required by privacy and data protection laws, obtaining explicit, informed and unambiguous consent from individuals at or before the time of collection. This includes informing individuals of their right to withdraw consent at any time and ensuring that consent is explicit, informed, voluntary, specific and current.

c) **Storage and security**: Taking reasonable measures to protect personal information from accidental or unlawful destruction, misuse, loss, alteration or unauthorised access or disclosure, and in accordance with the University's Information Security Policy.

d) **Use and disclosure**: Only using or disclosing personal information for the primary purpose for which it was collected, or another compliant purpose. Ensuring compliant privacy protections are in place when transferring personal information outside of Australia.

e) **Quality**: Taking reasonable steps to ensure personal information held by the University is accurate, complete and up to date.

f) **Access and correction**: Facilitating individuals seeking access to or correction of their own personal information, in accordance with the University's Freedom of Information (FOI) obligations.

g) **Anonymity and pseudonym**: Considering where lawful and practical, whether individuals can remain anonymous when conducting business with the University. Where full anonymity is not practicable, considering whether individuals can use pseudonyms to interact without revealing their true identity.

h) **Retention and disposal**: Destroying or permanently de-identifying personal information when no longer required for the purpose it was collected, in accordance with the University Records Retention & Disposal Authority.

5.4. All employees are required to complete mandatory information privacy compliance training (online module) upon onboarding and every two years thereafter.

5.5. Data and Privacy Impact Assessments (DPIAs) must be undertaken:

a) For any new technology or process intended to automate decision-making (fully or partially), including profiling, in a way that is likely to have significant impact on individuals;

b) When making changes to existing systems or activities, or using existing data, in a way that is likely to have significant impact on how personal information is processed; or

c) For any large-scale new project, initiative or process that involves processing a large volume of personal information.

5.6. DPIAs may be undertaken:

a) For any new IT system, project, initiative or process that involves the processing of personal information;

b) When conducting research that includes the collection, use, or sharing of personal information, especially if it involves new methodologies, technologies, or processing techniques that are likely to have significant impact on individuals; or

c) As directed by the PDPO or Privacy and Data Protection team.

5.7. The Privacy and Data Protection team must ensure privacy statements outlining how the University generally manages personal information are available on the University's public website.

5.8. Individuals can lodge a complaint with the University's Privacy and Data Protection team at privacy-officer@unimelb.edu.au, if they have concerns that their personal information has not been handled in accordance with the University's privacy obligations. Complaints must be investigated and the complainant responded to within a reasonable timeframe. More information, including how to contact the supervisory authority or regulator, is available on the University's website.

5.9. Suspected or actual privacy incidents must be promptly reported to the University's Privacy and Data Protection team and managed in accordance with the University's Process for Responding to a Privacy Incident (employee login required).

6. Roles and responsibilities

Role/Decision/Action	*Responsibility*	*Conditions and limitations*
Overall accountability for privacy compliance and contact point for relevant supervisory authorities and regulators.	Privacy and Data Protection Officer (University Secretary)	Operational support provided by Privacy and Data Protection team (Legal & Risk).
Oversee compliance with privacy and data protection laws, policies and processes, assessments, and audits.	Privacy and Data Protection Officer (University Secretary)	Privacy and Data Protection team monitor performance and report to the Privacy and Data Protection Officer.
Develop and maintain the University's Privacy Management Framework.	Privacy and Data Protection team (Legal & Risk)	
Conduct regular privacy assessments, audits and continuous improvement activities.	Privacy and Data Protection team (Legal & Risk)	Privacy and Data Protection Officer provides advice and oversight where required.
Inform and advise on privacy and data protection obligations and best practice.	Privacy and Data Protection team (Legal & Risk)	
Raise awareness and train all employees on privacy and data protection compliance and best practice.	Privacy and Data Protection team (Legal & Risk)	
Manage privacy enquiries, complaints, and incidents.	Privacy and Data Protection team (Legal & Risk)	Privacy and Data Protection Officer provides advice, and oversight where required.
Respond to requests from individuals to inform them about how their personal information is being used and what measures we put in place to protect their data.	Privacy and Data Protection team (Legal & Risk)	

Ensure that requests from individuals to access or amend their personal information, or to exercise other individual rights where applicable, are fulfilled or responded to appropriately.	Privacy and Data Protection team (Legal & Risk)	
Manage and maintain a central Privacy Collection Notice Register.	Privacy and Data Protection team (Legal & Risk)	
Promptly report any actual or suspected privacy incident to the Privacy and Data Protection team (Legal & Risk)	All employees	
Comply with the University's Privacy Management Policy.	All employees	
Complete mandatory privacy compliance training (online module) when required.	All employees	
Manage personal information in compliance with applicable privacy and data protection laws and community expectations. Where compliance requirements are unclear, seek guidance from the Privacy and Data Protection team.	All employees	
Create and maintain accurate and current Privacy Collection Notices for their functions or services.	All employees	

7. Definitions

Automated decision-making means a decision made either in a fully automated manner, without a human decision-maker ; or where a computer program substantially and directly informs or shapes the outcome, even if a human is involved in the final step of the process.

Controlled entity means an entity that is subject to the control of the University in terms of section 50AA of the *Corporations Act 2001 (Cth)* and includes an entity which is subject to the control of a controlled entity.

Employee means an individual employed by the University and is a national system employee within the meaning of the *Fair Work Act 2009* (Cth). Employee is also commonly referred to as staff member, academic staff member or professional staff member.

Health information means information or an opinion about a person's physical, mental or psychological health, any disability they may have, and any treatment they have received or wish to receive, that is also personal information. It includes genetic data that could be predictive of their or their family's health, and

personal information collected in relation to the provision of a health service or in connection with organ or tissue donation.

Information privacy means the policies, procedures, and other controls that establish how personal information or data is collected and processed.

International privacy and data protection law means any privacy and data protection law established outside of Australia that:

- may apply to the University's activities overseas; or
- may have extraterritorial scope and apply to the University's domestic activities in limited circumstances.

This includes the European Union General Data Protection Regulation (GDPR) 2016/679, UK GDPR (Data Protection Act 2018), and China's Personal Information Protection Law (PIPL) 2021.

Personal information or personal data means information that relates to an identified or identifiable (living) individual. It is information or an opinion about an individual whose identity is apparent or is reasonably ascertainable. For the context of this policy, 'personal information' includes personal, sensitive and health information.

Privacy impact assessment means a systematic assessment to identify potential privacy and data protection risks and recommendations to manage, minimise or eliminate them.

Privacy incident means when personal information held by the University is subject to misuse, loss, unauthorised access, modification or disclosure.

Privacy management means the program of activities adopted by the University to address privacy obligations and risks, as established by the University's Privacy Management Framework.

Privacy statement means the University's statements that explain generally what information the University collects and why, who we share it with, and how individuals can exercise their rights regarding their information.

Processing of personal data means all activities relating to its management by the University, from its collection and use, through to its storage and disposal, and everything in between.

Profiling means any form of automated or other processing of personal information used to evaluate certain personal aspects about an individual, such as their personality, behaviour, interests, habits, performance at work, economic situation, health, reliability, location or movements, in order to analyse, predict, or make decisions about them.

Sensitive information means information or opinion revealing an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs or affiliations, membership of a professional or trade association, membership of a trade union, sexual orientation ("sexual preferences or practices" in *Privacy and Data Protection Act 2014* (Vic)), or criminal record. International privacy and data protection laws, in addition to other privacy and data protection laws, can include additional categories of sensitive information with specific compliance obligations, such as genetic and biometric characteristics, financial accounts, and individual location tracking.

Supervisory authority or regulator means the authority or regulator of privacy compliance for a specific jurisdiction. This may include the Office of the Victorian Information Commissioner (in relation to personal information and/or sensitive information), Health Complaints Commissioner (in relation to health information), Office of the Australian Information Commissioner (to the extent that the Privacy Act 1988 (Cth)

applies) or other overseas privacy regulators (to the extent that international privacy and data protection laws apply).

POLICY APPROVER

Vice-President Administration & Finance and Chief Operating Officer

POLICY STEWARD

University Secretary

REVIEW

TBD

VERSION HISTORY

Version	Approved By	Approval Date	Effective Date	Sections Modified
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	TBD	TBD	TBD	Major amendments to reflect the University's Privacy Management Framework. Major review requirements met under Policy

				Framework (MPF1308).