PRIVACY POLICY

Section	University Management
Contact	Director Governance and Assurance
Last Review	August 2025
Next Review	August 2023
Approval	SLT 25/08/79
Effective Date	August 2025

PURPOSE

The purpose of this policy is to support all members of the university in handling personal information responsibly, in line with the Privacy Act 2020 other applicable legislation, and to ensure the University meets it's stated commitments to individuals about how their data will be used and protected.

This policy should be read alongside the university's Privacy Notices and is supported by a set of privacy procedures, guidelines and associated documents which form the university's Privacy Framework.

POLICY

1. Collection of personal information

    1.1. The university will collect personal information only where it is necessary to do so for a lawful purpose associated with normal university functions and activities, including where required to do so for reporting purposes.

    1.2. The university will collect personal information directly from the individual concerned where it is practical and reasonable to do so unless an exception applies or unless the individual concerned consents otherwise.

    1.3. The university collects information by various means and for a variety of purposes, and is required to be transparent about how, when, and why it collects personal information. To achieve this transparency, the university will maintain and publish Privacy Notices which make people aware of the collection of their information, the purpose for doing so (including intended usage and disclosure), and the rights of individuals in respect to access and correction of their information.

    1.4. The Privacy Notices will be published online at http://www.massey.ac.nz/massey/privacy on university websites and/or linked to systems or forms that collect and store personal information.

    1.5. Collection, use and disclosure of personal information by the university (including people and processes and systems) must comply with the Privacy Notices.

2. Storage and security of personal information

    2.1. Personal information, where classified as a record, will be retained, and stored in accordance with the Information and Records Management Policy and Procedures.

    2.2. Access to personal information, will be granted in accordance with the established approval processes for each system and/or data repository, and shall only be granted if required as part of a staff member's role.

2.3. All systems must comply with the Information and Technology Security Policy including all security roles and responsibilities assigned to data leaders, data custodians and data stewards.

3. Requests for access to and correction of personal information and other Data Subject Rights Requests

3.1. Routine requests covered by an approved standard operating procedure, should be responded to by the operational group in receipt of the request.

3.2. Non-routine requests must be reported to the Privacy Officer for processing (as appliable) in accordance with the procedure outlined in the Responding to a Privacy Request guidelines.

3.3 If the university declines to amend a person's personal information following a correction request, it must inform the person of their right to have their request and the university's refusal noted on their personal file. If a person decides to exercise this right, then the university must note the person's request and the university's refusal on the person's personal file.

3.4 Any Data Subject Rights requests issued to the university under any global privacy legislation should be referred to the Privacy Officer for assessment prior to responding.

4. Accuracy of personal information

4.1. The university will take reasonable steps to ensure, prior to its use, that the information is correct, complete, and up to date.

5. Retention of personal information

5.1. Records containing personal information will be destroyed confidentially in accordance with the General Disposal Schedule (GDA), and the university's own procedures. Personal information collected that is not a Record requiring retention under the Public Records Act should be disposed of when it is no longer needed i.e., when the purpose for which it was collected has expired.

6. Use and disclosure of personal information

6.1. The university will not disclose personal information for a purpose that is not consistent with that for which it was collected, unless required or permitted to do so by law, or consent has been obtained from individuals for their information to be disclosed for certain other purposes.

6.2. University staff must only access and/or use personal information where required to carry out a function of their employment with the university. In accordance with the Act, staff must also ensure:

(i) They do not disclose any personal (student or staff) information to another staff member unless that staff member also has a professional need to use the information.

(ii) They do not disclose any personal (student or staff) information to another individual or organisation external to the university, unless authorised to do so.

7. Disclosure outside New Zealand

7.1. The university will only disclose an individual's personal information to another organisation or person outside New Zealand if that organisation or person:

(i) is an agent of the university and the information is being sent to the agent for storage or processing and the agent does not use or disclose the information for its own purposes.

(ii) is the personal representative of the individual concerned;

(iii) is subject to the Privacy Act because they are a New Zealand agency (with an overseas office), or they are an overseas agency doing business in New Zealand;

(iv) agrees to protect the information in such a way to provide comparable safeguards to the Privacy Act, e.g.by using model (or other appropriate) contract clauses; or

(v) is subject to privacy laws that provide comparable safeguards to the Privacy Act.

7.2 The transfer of personal information out of New Zealand by the university must comply with New Zealand legislation.

8. Using unique identifiers

8.1. A unique identifier will be assigned to each student, which will be used in conjunction with a secondary means of identification or password/PIN. Staff must also take reasonable steps to protect unique identifiers from misuse and make sure they verify someone's identity before assigning a unique identifier.

9. Privacy Impact Assessments

9.1. A Privacy Impact Threshold Assessment must be completed for any project or change that affects personal information about university data subjects to determine whether a Privacy Impact Assessment ("PIA") is required. A PIA must be completed for any project or change where the assessment indicates it could be high-risk from a privacy perspective.

9.2 PIAs require Privacy Officer sign-off and the policy owner, process owner or project sponsor (as applicable) is accountable for undertaking the Privacy Impact Threshold Assessment and for ensuring the implementation of any agreed recommendations resulting from a PIA.

10. Responsibilities

10.1 All university members must:
- (i) understand and comply with the Privacy Framework
- (ii) actively participate in any privacy training provided by the university, and
- (iii) keep their manager and/or the Privacy Officer informed of any Data Subject Rights Request, privacy breaches or other privacy issues.

10.2 Managers must:
- (i) support staff to understand and comply with this policy and participate in any privacy training provided by the university, and
- (ii) ensure Data Subject Rights Requests, privacy breaches and other privacy issues are identified and managed in accordance with the Privacy Framework.

10.3 The Privacy Officer must:
- (i) support all university members to understand and comply with the Privacy Framework, including by maintaining and developing relevant procedures, standards and guidelines
- (ii) assist with the management of Data Subject Rights Requests, privacy breaches and other privacy issues by university members
- (iii) assist with the management of privacy complaints from data subjects
- (iv) report on privacy breaches and general privacy compliance to the Vice-Chancellor,

and

(v) liaise with third parties in respect of privacy matters, including the Privacy Commissioner or other relevant regulators and data subjects.

11. Privacy Officers

11.1 The Privacy Officers for the university are appointed by the Vice-Chancellor. The Privacy Officer for staff is the Director Employment Relations & Advisory and for all other matters is the Director of Governance and Assurance.

11.2 The Privacy Officers will receive all requests for information, notification of privacy breaches and complaints. Investigation of breaches and resolution of privacy related complaints is undertaken by the Privacy Officer or their delegates.

SCOPE

This policy applies to all university staff, contractors and students who interact with all university campuses in New Zealand, on-line, and worldwide.

The policy also applies to wholly owned subsidiaries and controlled entities of the university, as is required by the Controlled Entities Governance Framework Policy.

This policy is not intended to be a stand-alone document. It must be read and applied in conjunction with:

- The agreements between Massey University and its staff.
- The agreements between Massey University and its students.
- The agreements between Massey University and its contractors.
- The Privacy Management Framework.
- Massey University Privacy Notices.
- All relevant law, including the Privacy Act 2020.

DEFINITIONS

Data Subject: means any natural person about whom the university collects and holds personal information and includes students, staff, contractors, alumni, donors, research participants, and visitors to the university's websites or campuses.

Data Subject Rights Requests: means in addition to access and correction requests under the Privacy Act, any data subject rights under various global privacy legislation that the university may also be bound to respond to.

Personal Information: means any information, whether electronic or hard copy, about a data subject, whether or not the information directly identifies the data subject, and includes but is not limited to contact, demographic, health and academic information (including course results), CCTV footage, staff performance information, emails and other correspondence, and opinions about the data subject.

Privacy Framework: means this policy and any procedures, standards or guidelines issued to support it, including but not limited to the Responding to a Privacy Request Process, Data Breach Notification Procedures, Privacy Impact Assessment Process, and other business unit or process specific privacy guidelines/authorised standard operating procedures.

Privacy Impact Assessment "PIA": is a process that helps identify the potential effects a change may have on personal information. The PIA process is about ensuring that a change does not impact on the university's ability to

comply with the Privacy Act 2020 and where applicable other global privacy obligations. It helps the university deliver new products, services or processes in a way that protects the privacy of its data subjects.

Privacy Impact Threshold Assessment is step 1 of the Privacy Impact Assessment process for deciding whether the change or project is high risk from a privacy perspective.

RELEVANT LEGISLATION

Privacy Act 2020
Official Information Act 1982
Health Information Privacy Code 2020 Public Records Act 2005
Education (Pastoral Care of Tertiary and International Learners) Code of Practice 2021

LEGAL COMPLIANCE

Collection, use and disclosure of personal information, and access to and correction of personal information and the use of unique identifiers, must comply with the principles of the **Privacy Act 2020.** The university must appoint a 'Privacy Officer' with responsibilities for compliance with these principles, and to handle requests for access.

Requests made under the **Official Information Act 1982** by an individual requesting information held about themselves, is deemed to be a request made pursuant to ss 1(b) Principle 6 of the Privacy Act 2020. Requests for personal information about persons other than the requestor will be considered under the Official Information Act 1982.

Specific units within the university are health agencies and are obliged to comply with the requirements of the **Health Information Privacy Code 2020.** This code requires the University appoint a 'Privacy Officer' with responsibilities for compliance with these principles, and to deal with requests for access. Access to all Health Information for identified individuals must be secured.

Personal information must also be retained and stored in compliance with the **Public Records Act 2005** and the records containing such personal information must be destroyed confidentially in accordance with the General Disposal Schedule (GDA),

Additional global legal compliance obligations must at times also be complied with according to the region a Data Subject is located in at the time of collection of the Personal Information. Further information related to this is detailed in the University Privacy Notices as updated from time to time.

RELATED PROCEDURES / DOCUMENTS

Massey University Privacy Notice
Privacy Impact Assessment Process
Responding to a Privacy Request
Data Breach Notification Procedures
Data Management Policy
Information and Records Management Policies and Procedures
Information and Technology Security Policy

DOCUMENT MANAGEMENT CONTROL

Owned by: Director Governance and Assurance Authorised by: SLT
Date issued: 24 May 2006
Last review: August 2025
Next review: August 2030