PRIVACY POLICY

Section	University Management
Contact	Director Risk and Assurance
Last Review	September 2017
Next Review	September 2022
Approval	C18/09
Effective Date	July 2014

PURPOSE

The purpose of this policy is to ensure that Massey University maintains privacy management practices that:

a) Comply with the Privacy Act 1993, and the 12 Privacy Principles included therein;
b) Promote a culture that protects and respects private information;
c) Educate people within the University about information privacy; and
d) Monitor privacy compliance and support the development of systems and process that ensure privacy by design.

POLICY

Policy statements are provided for each of the four desired outcomes as follows:

Comply with the Privacy Act 1993, including the 12 Privacy Principles

1. Collection of personal information (principles 1-4)

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 Statements 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 Statements will be published in the University Calendar, online at http://www.massey.ac.nz/massey/privacy on University websites and/or linked to systems that collect and store personal information, such as: Student Enrolment System; STREAM; Massey Contact Systems; Staff recruitment website; Alumni website; Library website; and HR systems.

1.5. The Privacy Statements will be consistent at all times with this Policy, demonstrate good privacy management practice, will be maintained and fit-for-purpose at all times.

1.6. Collection, use and disclosure of personal information by the University (including people and processes and systems) must comply with the Privacy Statements.

2. Storage and security of personal information (principle 5)

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. Business system owners must also ensure that personal information stored is protected from loss, misuse, or inappropriate disclosure, and maintain appropriate levels of access and system security, including ensuring that access to personal information is removed when no longer required by a role or individual. At all times business systems must comply with the security requirements or directives of ITS.

2.4. Security of University networks will be maintained by ITS.

2.5. Where systems containing personal information are planned, implemented, or significantly upgraded, a Privacy Impact Assessment must be undertaken. The transfer of personal information out of New Zealand by the University must comply with New Zealand legislation and good practice. A Privacy Impact Assessment must be undertaken for any proposed developments where personal information is to be transferred overseas, including use of cloud based services.

3. Requests for access to and correction of personal information (principles 6 and 7 plus parts 4 and 5 of the Act)

3.1. The University acknowledges that unless an exception applies, individuals have the right to access their personal information, and the right to request correction of information.

3.2. Any staff member, student (including prospective student, graduate and alumni where the context applies), member of the public or their agent may request access to personal information about themselves held by the University.

3.3. Where such a request is covered by an approved standard operating procedure and is a routine request, the operational group in receipt of the request should respond.

3.4. Non-routine requests, and those not covered by approved standard operating procedures must be reported to the Privacy Officer and will be handled in accordance with the procedure outlined in the Guidelines for dealing with requests and corrections to personal information.

3.5. Anyone is entitled to request correction of their own personal information. Where such a request is made the University must decide whether or not to correct the personal information. Once it has decided the University must inform the requestor of its decision. If the University declines to amend the person's personal information, 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.

4. Accuracy of personal information (principle 8)

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 (principle 9)

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 (principles 10 and 11)

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. Using unique identifiers (principle 12)

7.1. A unique identifier will be assigned to each student, which will be used in conjunction with a secondary means of identification or password/PIN.

Promote a culture that protects and respects private information

To promote and encourage a culture that protects and respects private information the University endeavours to model high standards of privacy practice and ensure that respect for the privacy of individuals is inherent in the operations of the University. Robust privacy practice will be ensured through the following:

1. Management of Privacy breaches

All privacy breaches must be reported to the Privacy Officer. A record of privacy breaches, and their remediation, will be maintained by the Privacy Officer (or delegate). Privacy breaches must be remedied as soon as possible in consultation with the section where the breach occurred, Risk and Assurance and the Privacy Officer.

2. Responding to Privacy Complaints and investigations by the Privacy Commissioner

All complaints received must be reported to the Privacy Officer who may delegate the responsibility for investigation and management of the complaint. Complaints will be managed promptly and remedied as quickly as possible. Legal advice may be sought in respect of complaints that escalate to the Privacy Commissioner. Any complaint resulting in a settlement must be approved by the Vice-Chancellor.

3. All staff having a responsibility to:
- maintain good practice privacy behaviours
- report all privacy breaches to the Privacy Officer
- understand and comply with obligations in regard to privacy, relevant to their position
- report and/or escalate concerns or issues relating to privacy
- ensure they are appropriately trained and/or informed of privacy handling practices relevant to their work

The Privacy Officer for the University, with responsibilities for legislative compliance, is appointed by the Vice-Chancellor and is the AVC Operations, International and University Registrar.

The Privacy Officer 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 Director Risk and Assurance.

Educate people within the University about information privacy

An annual programme of awareness building and skills training will be provided to staff. The Privacy Policy and best practice privacy management practices adopted by the University, will be promoted to staff annually.

Staff managing systems (Business system owners) and data stewards must attend privacy training to ensure that their skill set and understanding is current and up-to-date. Staff operating and accessing such systems are strongly encouraged to attend privacy training or to complete an online privacy training module as part of their induction.

Systems that hold personal information shall incorporate aspects of best practice Privacy management into their training and induction materials, consistent with this Policy and the University's Privacy Statements.

Monitor privacy compliance and support development of systems and processes that ensure privacy by design

Reports will be provided by the Privacy Officer, or delegate, on progress against any specific privacy management workplans, breaches and complaints, as required or requested.

Compliance with the Privacy Act 1993 will be reviewed in conjunction with the Legislative Compliance Process each year, and all non-compliance will be reported.

Where systems containing personal information are planned, implemented, or significantly upgraded, a Privacy Impact Assessment must be undertaken. The transfer of personal information out of New Zealand by the University must comply with New Zealand legislation and good practice. A Privacy Impact Assessment must be undertaken for any proposed developments where personal information is to be transferred overseas (including use of Cloud based services).

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.

Specific units within the University are effectively health agencies and are obliged to comply with the requirements of the Health Information Privacy Code 1994.

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

- The Information Privacy Principles in the Privacy Act 1993.
- 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 Statements
- All relevant law, including the Privacy Act 1993.

DEFINITIONS

Personal Information: is any information, on its own or combined with other information, about an identifiable individual.

Privacy Impact Assessment: is a systematic process for evaluating a proposal in terms of its impact upon privacy used to identify the potential effects that a proposal may have upon individual privacy, examine how any detrimental effects upon privacy might be overcome and ensure that new projects comply with the information privacy principles.

AUDIENCE

This Policy applies to all University staff and students who interact with Massey University campuses in New Zealand, on-line, and worldwide, including wholly owned subsidiaries and controlled entities of Massey University, as is required by the Controlled Entities Governance Framework Policy.

Specific units within the University are effectively health agencies and are obliged to comply with the requirements of the Health Information Privacy Code 1994.

RELEVANT LEGISLATION

Privacy Act 1993
Official Information Act 1982
Health Information Privacy Code 1994
Public Records Act 2005

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 1993**. 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 1993. Requests for personal information about persons other than the requestor will be considered under the Official Information Act 1982.

The **Health Information Privacy Code 1994** 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),

RELATED PROCEDURES / DOCUMENTS

Data Management Policy
Massey University Privacy Statements
Privacy Impact Assessment
Guidelines for dealing with a request or correct to personal information
Information and Records Management Policies and Procedures

DOCUMENT MANAGEMENT CONTROL

Owned by: Assistant Vice-Chancellor Operations, International and University Registrar

Authorised by:
Date issued: 24 May 2006
Last review: September 2017
Next review: September 2022