PRIVACY MANAGEMENT FRAMEWORK

Section	Office of the AVC Operations, International and University Registrar
Contact	Risk Management
Last Review	July 2014
Next Review	July 2017
Approval	SLT14/7/176
Effective Date	July 2014

PURPOSE

Massey University values the privacy of every individual's personal information and is committed to the protection of personal information.

Privacy @ Massey University:

Massey University has established a privacy regime which aims to;

- Develop and promote a culture that protects and respects private information.
- Educate people within the University about information privacy.
- Monitor privacy compliance and support the development of systems and process that ensure privacy by design.

This Privacy Management Framework outlines the core purpose, principles, policy, roles and responsibilities, and mechanisms for oversight, incident management and reporting.

Massey University aims to comply with the Privacy Information Principles of the Privacy Act 1993, and the Health Information Privacy Code 1994 as stated in the Massey University Privacy Policy.

The University Privacy Officer, can be contacted at:

Privacy Officer
Office of AVC Operations, International and University Registrar
Massey University
University House
Private Bag 11 222
Palmerston North 4440
Phone: 06 356 9099
Email: privacy.officer@massey.ac.nz

SCOPE

The Privacy Management Framework applies to all University staff and students who interact with Massey University campuses in New Zealand, on-line, and worldwide.

The Privacy Management Framework applies to 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.

DEFINITIONS

Student ID: a unique identifier assigned by Massey University to students.

Health Information Identifier: an identifying name or code (usually a number) assigned by an organisation to an individual in connection with that person's health information.

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

Primary Purpose: the purpose for which the information is collected. This is directly related to the core function or activity e.g. student enrolment.

Secondary Purpose: when the information is used for another purpose than the primary purpose. The secondary purpose for which the information is collected must be connected or associated with the primary purpose. If sensitive information is involved, it must be directly related to the primary purpose.

Sensitive Information: Information or an opinion about an individual including, but not limited to:

- Racial or ethnic origin
- Political opinions
- Membership of a political association
- Religious beliefs or affiliations
- Philosophical beliefs
- Membership of a profession or trade association
- Membership of a trade Union
- Sexual preferences or practices
- Criminal record
- Health information
- Contact details
- Employee or student performance

PRIVACY GOVERNANCE

Massey University is committed to complying with its obligations in respect of personal information under the Privacy Act 1993, and the Official Information Act 1982, and related Health Information Privacy Code 1994. This commitment is stated in the Massey University Privacy Policy approved by Council.

ROLES AND RESPONSIBILITIES

Chancellor and Council will:

- approve the Privacy Policy, and be responsible for oversight of compliance with the University's policy and procedures.
- receive periodic reports on the outcomes of the Privacy Management Programme of Work, and summarised notification of privacy breaches, and resultant action.
- delegate to the Vice-Chancellor in accordance with the Education Act 1990.

Vice Chancellor and members of the Senior Leadership Team (SLT) will:

- endorse the Privacy Policy, and Privacy Management Framework, and approve the Privacy Management Programme of Work that supports the implementation of the Framework.
- receive periodic updates on the Privacy Management Programme of Work, and notification of privacy breaches, complaints and their outcomes, including any complaints which are considered to pose risk of legal action against Massey University.
- model best privacy practices and ensure respect for the privacy of individuals is core to all aspects of the University's culture.

Privacy Officer:

The Vice-Chancellor will appoint the University Privacy Officer, who will be a senior member of staff, and the Privacy Officer will:

- develop and manage the Privacy Management Workplan.
- respond to requests for information and receive all complaints.
- be responsible for the provision of information, investigation of privacy breaches and resolution of complaints made under the Privacy Act 1993. These may be sub-delegated by the Privacy Officer.

Heads of Departments (or equivalent) will:

- model good privacy behaviour by demonstrating sound judgement in privacy matters
- comply with legislative requirements

- ensure privacy breaches and near misses are accurately recorded, reported to the Privacy Officer and investigated,
- identify privacy risks
- ensuring training is provided for staff.

Risk Management Office:

In conjunction with the Privacy Officer the Risk Management Office will

- develop, implement and continuously improve the Privacy Management processes
- identify compliance obligations and risks relating to privacy in conjunction with managers
- undertake Privacy Impact Assessments
- advise on integration of privacy risk management within relevant policies and procedures, and business processes
- support training for managers in regard to privacy
- develop mechanisms for reporting of privacy management to senior management and Council,
- respond to requests for personal information made under the Privacy Act
- deal with privacy incidents as the Delegate of the Privacy Officer.

Information Technology Services will:

- ensure that access controls are developed, implemented, maintained and with appropriate logging
- proactively manage security to all data and information on the Massey University network from accidental and malicious access
- develop and maintain an information asset register that identifies all the data assets, who is responsible for managing them and which are repositories of personal information

Authorised University Staff:

Where information is collected in relation to the employment of staff such information may be used in aggregated form for the purposes of financial, workforce planning or other employment related matters by staff authorised by the University to carry out such work.

All Staff will:

- maintain best practice privacy behaviours
- promote privacy at work
- actively participate in privacy training
- report all privacy breaches and near misses to managers
- identify privacy risks and observe obligations in regard to privacy, relevant to their position
- undertake training as required
- identify and report and/or escalate concerns, issues, or privacy breaches

PRINCIPLES OF GOOD PRIVACY MANAGEMENT

Personal information is any information about an identifiable living individual. It can include opinion, and could be information recorded in any format, including a database, the information may or may not be true, and it may also be Sensitive Information.

Massey University collects information by various means and for a variety of purposes associated with the University's purpose of teaching, research and community service and in relation to employment with the University.

Accordingly, Massey University will ensure that:

- the purpose for which personal information is collected is transparent
- the organisations with whom Massey University shares information are identified
- any legislation that requires Massey University to collect personal information is known
- consequence for individuals who provide or receive information in error is documented and available
- privacy training, advice and support is provided
- a process exists for continuous improvement of systems and processes in respect of protecting personal information
- a documented process is in place to advise and resolve privacy breaches and respond to requests for personal information

Monitoring and Compliance

Oversight of Privacy Risk Management is the responsibility of the Vice-Chancellor, who will designate a senior staff member as Privacy Officer of the University. Reports will be provided by the Privacy Officer, or delegate, of progress on the Privacy Management Workplan, breaches and complaints, on not less than an annual basis.

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.

Privacy Risk Management

A Privacy Impact Assessment will be undertaken when systems containing personal information are implemented, or significantly upgraded.

Collection of personal Information

To the extent required by the Privacy Act 1993, Massey University will collect information only for the purposes linked to the University's purpose of teaching, research and community service, or in relation to employment.

Massey University will collect information directly from the individual where it is practical and reasonable to do so. Where the University collect information from an authorised third party (e.g. Agent, other TEI, Government Agency), the University will take reasonable steps to ensure the individual is aware that this information has been provided.

Massey University is required to collect information for reporting purposes e.g. Government statistical reports. Accordingly Massey University will publish Privacy Statements which make people aware of the collection of information, our purposes for doing so, and the rights of individuals.

Privacy Statements will be published on systems that collect and store personal information of any type. These include but are not limited to:

- Massey University websites
- Student Administration systems, including on-line enrolment
- Massey Contact systems
- STREAM
- Staff Recruitment websites
- Alumni Development websites
- HR systems

Such statements will be consistent with the University's Privacy Policy, demonstrate good privacy management practice, and will be maintained up-to-date, and fit-for-purpose at all times.

Record Keeping, Storage and Retention of personal information

Personal information will be retained and stored in accordance with the Record Management Policy and Procedures. Access will be restricted to authorised persons, and will be periodically reviewed. Records containing personal information will be destroyed confidentially in accordance with the General Disposal Schedule (GDA), and Massey University's own procedures.

Security and quality of personal information

Massey University will collate and maintain an Inventory of Repositories of Personal Information (PII) and will aim to ensure that the information contained is protected from loss, misuse, or inappropriate disclosure. Processes to ensure authorised access will be implemented, and periodically reviewed.

Inventories may be either paper based, or electronic, and may contain personal information in form of, or combination of, text, data, and/or graphics or images.

Access to, Use and Disclosure of personal information

The University acknowledges that individuals have the right to access their personal information, and the right to amend information that is factually incorrect.

Massey University is committed to only use personal information for the purpose for which it was collected, and will take reasonable steps to ensure that the information is correct, complete and up-to-date.

Massey University will not disclose personal information for a purpose that is not consistent with that for which it was collected, unless required to do so by law, or if written consent has been obtained from individuals for their personal information to be used, or disclosed for certain purposes.

Trans-border data flows

Transfer of personal information out of New Zealand by the University must comply with New Zealand legislation and good practice. Any proposed developments where personal information is to be transferred overseas will require a Privacy Risk Assessment before implementation.

PRIVACY INCIDENT MANAGEMENT

Management of requests for personal information

Requests for personal information will be receipted on request and sent directly to the section which holds the relevant information. Responses must be answered within 20 working days from the date of receipt, unless there is a good reason this cannot be provided within the stipulated period, in which case an extension may be requested.

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 will be remedied as soon as possible and in accordance with the Privacy Incident Management Process.

Responding to Privacy Complaints

All complaints received must be reported to the Privacy Officer who will delegate the responsibility for investigation and management of the complaint. Complaints will be managed promptly and remedied as quickly as possible. All complaints are to be recorded by the Privacy Officer (or delegate).

Legal advice will be sought in respect of complaints that escalate to the Privacy Commission.

Any complaint resulting in a settlement must be approved by the Vice-Chancellor.

Privacy Awareness and Training

An annual programme of awareness building and skills training will be prepared and delivered. This may include any or a combination of the following;

- electronic newsletters
- face-to-face training events
- resource kits
- intranet based information

Staff managing systems (data owners and data stewards) identified in the Inventory of Repositories of Personal Information must attend privacy training to ensure that their skills set and understanding is current and up-to-date. Staff operating such systems are strongly encouraged to attend privacy training.

Attendance at privacy training will be recorded on the training and development database retained by People and Organisational Development.

AUDIENCE

All Staff

RELEVANT LEGISLATION

Privacy Act 1993
Official Information Act 1982
Health Information Privacy Code 1994

LEGAL COMPLIANCE

Privacy Act 1993
Procedures for collection, use and disclosure of personal information about identifiable individuals, and access to and correction of personal information and the use of unique identifiers, must comply with the twelve 'Privacy Principles of Privacy Act 1993. Massey University must appoint a 'Privacy Officer' with responsibilities for compliance with these principles, and to deal with requests for access.

Official Information Act
All requests made under the Official Information Act 1982 are deemed to be a request made pursuant to with ss 1(b) Principle 6 of the Privacy Act 1993.

Health information Privacy Code 1994 requires that Massey 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.

RELATED PROCEDURES / DOCUMENTS

Procedures for the Collection, Use and Disclosure of Personal Information
Privacy Incident Management Process
Privacy Impact Assessment Toolkit
Privacy Statements – Appendix A
Records Management Policy and Procedures

DOCUMENT MANAGEMENT

Prepared by:	Risk Manager
Authorised by:	AVC Operations, International and University Registrar
Approved by:	SLT14/7/176
Date issued:	July 2014
Last review:	July 2014
Next review:	July 2017

APPENDIX A

STANDARDISED UNIVERSITY PRIVACY STATEMENTS

Privacy of Personal Information – Students (long format)

For use in: *University website (url: http://privacy.[university].ac.nz)*
University Calendar

[University] will collect, use, store, and disclose personal information relating to students in accordance with the provisions of the Privacy Act 1993. Where practicable all such personal information is obtained directly from students, or from their nominated agent(s). Additionally, information may be obtained or verified through relevant government or education agencies, including the New Zealand National Student Index.

Information will be stored on University files and database(s) and all reasonable security measures will be maintained. 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 members and other personnel within the University or within agencies under contract to the University will have access to students' personal information for purposes relevant to normal university operations including but not limited to: admission, enrolment, study, academic progress, attendance and participation in learning events and activities, tuition fees and charges, establishing and maintaining academic and graduation records, assessment, academic agreements (exchange/ study abroad partners, scholarship providers or sponsors, programme delivery partners), academic advice & support, student services, discipline, security and safety, Library and IT services, managing students' association(s) membership and records, managing records of graduates, and other alumni, and managing and improving the quality of services provided by the University.

In order to conduct its proper business and as required under the Education Act 1989 and other laws, regulations, and contractual agreements by which it is bound, the University may use the student information it holds and may disclose information to external agencies such as government departments, bodies responsible for course moderation and professional accreditation or membership, agencies for financial support and pastoral care, and university student and alumni associations.

Such agencies may include, but are not limited to:

- The Ministry of Education (information will be recorded on the National Student Index and used in an authorised information matching programme with the NZ Birth Register)
- The Ministry of Social Development (including Work and Income NZ and StudyLink)
- Inland Revenue Department
- Te Puni Kōkiri
- Immigration New Zealand (for students who are not NZ citizens)
- Relevant Professional bodies
- Course moderation or accreditation bodies
- Tertiary Education Commission
- Ministry of Trade and Enterprise
- Education New Zealand

Information provided to external agencies is either student specific (typically name, date of birth, current contact details and academic/ graduation details) or cohort specific (aggregated or statistical information that does not identify individuals).

Where provision or disclosure of information is voluntary or falls outside the scope of information the University is permitted to collect, store, use and disclose under the Privacy Act 1993, students will be advised and their consent will be obtained prior to the provision or disclosure of information.

The University will make information held about students available to them upon request and in accordance with the Privacy Act 1993, which also describes the conditions under which information may be withheld. Students have the right to request correction of personal information held in accordance with the provisions of the Privacy Act 1993. If a student withholds information or provides incomplete, false or misleading information the University may decline or cancel the admission or enrolment and may withhold the academic record if its veracity cannot be confirmed.

This privacy statement operates in conjunction with any other privacy statement.

Privacy of Personal Information – Students (short format)

Unrestricted Use

[University] collects, stores, uses and discloses personal information relating to students in accordance with the Privacy Act 1993 for the purpose of conducting its proper business. A unique identifier is assigned to each student. Personal information is disclosed to other agencies as required under the Education Act 1989 and other relevant New Zealand laws, regulations, and contractual agreements by which the University is bound. Students have the right to access and seek correction of their personal information. More information on the University's protection of the privacy of personal information is available at [http: //privacy.[university].ac.nz and in the University Calendar.

Student Declaration

For use in: *Enrolment Application*
Admission Application (if separate)

I understand that [University] will collect, store, use and disclose personal information about me in the course of conducting its proper business and that a unique identifier will be assigned to me to facilitate this. I have read and understand how such information will be managed and disclosed in accordance with the Privacy Act 1993, and as outlined on the University website (http://privacy.[university].ac.nz) and in the University Calendar. I acknowledge that I have the right to access and seek correction of personal information about me and understand that if I withhold information or provide false or misleading information my enrolment may be terminated.