Advising and Communications
Privacy Guidelines
April 2023

1. Purpose

The purpose of this document is to establish guidelines for staff in response to requests were access to personal information is received.

We provide a range of services, from a prospective student initial inquiry through to their graduation and beyond. For this reason, staff have access to a large amount of personal information.

The Privacy Act 2020 and the EU General Data Protection Regulations (GDPR) provide the legislative context for the protection and use of personal information. The following guidelines are intended to interpret the legislation in the context of the role and responsibilities of staff, to assist them to provide adequate security for this information.

2. Policy

Refer to the Massey University Privacy Policy in Appendix 1 or see **https://masseyuni.sharepoint.com/sites/RiskAssurancePoliciesProcedures/Shared Documents/Forms/AllItems.aspx?id=%2Fsites%2FRiskAssurancePoliciesProcedures%2FShared Documents%2FPrivacy_Policy%2Epdf&parent=%2Fsites%2FRiskAssurancePoliciesProcedures%2FShared Documents&p=true&ga=1**

3. Audience

All staff within Advising and Communications at Massey University.

4. Personal Information Access and Correction Requests

Staff have access to a large amount of personal information to provide a complete and accurate service to Massey University students. Personal information is usually stored and retrieved with the use of an ID number or any of the contact methods used, for example personal information can be stored in various media either electronically including voice and screen recordings, text messages, email message, chat transcripts, social media messages, facsimile, notes entered in the Customer Relationship Management (CRM) system and the like, or via more traditional methods such as written correspondence.

Subject to some exceptions, any information that is classified as personal is only able to be accessed or maintained either by the individual themselves, or by an authorised agent. In this case the individual is a Massey student and the authorised agent is a person employed or otherwise bound to Massey University and who is specifically authorised to access that information or an authorised agent of the student themselves.

Requests for access to or correction of private information can be either verbal or written. A request does not have to be in writing. Staff are agents of the University and can release or correct personal information instantaneously (including live playback of voice recordings to callers) once the identity and procedures in Section 5 have been confirmed. If further assistance is required, staff are to seek the assistance of their line manager or direct the enquiry to the University's Privacy Officer in Section 14 of this guideline (you may be able to withhold information

in certain situations). A request for access to or correction of personal information made under Principle 6 or 7 of the Privacy Act must be responded to as soon as possible and within 20 working days and if the information should be provided then this must be provided without undue delay.

However, different timelines and requirements may apply if the request received relates to information that Massey University processed while the student was physically present in the EU as the request may be covered by the requirement of the GDPR.

4B. GDPR Requests

The GDPR regulations specify 11 specific rights an individual has in regard to personal information collected and stored about them (including the right of access and correction) as follows:

I. Right to basic information
II. Right of access
III. Right of rectification
IV. Right of erasure ("Right to be Forgotten")
V. Right to restrict processing
VI. Right to data portability
VII. Right to object to processing
VIII. Rights related to automated decision making and profiling
IX. Right to breach notification
X. Right to lodge a complaint
XI. Right to compensation

The processes for ensuring Massey complies with the GDPR are still under development. If a staff member is advised or has any reason to suspect that a caller's or requestor's enquiry or request is covered by the GDPR they should escalate the request to their line manager who may in turn need to review the request with the Governance and Assurance Office.

Examples of where this may be applicable are:

- The caller or requestor may make reference to the GDPR or the rights the regulations provide them with
- The caller or requestor advises that they are studying by distance or onshore from a country in the EU
- The staff member ascertains that the caller or requestors current address or country of domicile is within the EU
- The caller or requestor may be calling from a country from within the EU
- The requestor may be emailing Massey University from an EU email address
- The caller or requestor may phrase their request in language that leads the staff member to suspect that the request could be subject to the regulations for example they may for example use the term "erasure' or "right to be forgotten" etc.

5. Guideline for Releasing Information to Individuals

Information is collected for the purposes of studying at Massey University and/or as set out in the University's privacy statements https://www.massey.ac.nz/massey/privacy.cfm. Staff must ensure that information is only released to the student to whom it belongs, (with some exceptions as contained within the Privacy Act and the GDPR) and that only the student makes changes to existing information. This responsibility is carried out by performing a suitable **check on the identity of a customer before releasing or altering any personal information.**

A suitable check is defined as obtaining a correct response from the student directly to confirm their identification number (if known) and **all** of the following:

- Current Address or Email Address
- Date of Birth
- Full Name (as shown on the birth certificate or passport).

If providing face to face assistance, photo identification is acceptable. If staff are in doubt about the photo ID on file matching the student, the above questions should also be asked.

(Note: It is advisable to obtain an ID number from the student, rather than searching for it via CRM and the student portal because the number of identifiers available is reduced.)

If staff are in any doubt as to the identity of the customer, including if they are unsure about the photo ID, other questions should be used, possibly drawn from their academic details: for example, the numbers/titles of the last three courses that the student was registered in.

If doubt still exists, do not release the information.

Staff can assume, having performed this check on the identity of the caller, that the caller is being truthful about their identity. In other words, staff will not be considered negligent in discharging their responsibility for protecting the information if they are dealing with a person who has answered all questions correctly.

6. Receiving and uploading and sending documents

The current practice for accepting and uploading documents is based the ID number if it is provided, or if we can locate the student record via their email address, full name and date of birth, this is sufficient for uploading a document or sending it on to the appropriate department.

Documents can be received by a student or third party and uploaded if the correct student file can be located by the above practice.

When sending a document to a customer we need to ensure that we clearly label these documents using the students name, identification number and the document type e.g., Jane Smith ID 12345678 Academic Record. Where there maybe more than one Academic Record document you will add a 1, 2, 3 etc. to the end of the document type, for example Academic Record1.

A check must be done when reviewing your final content, make sure the name and ID of the attachment match your intended recipient.

These documents can be saved to your desktop.

After every interaction, staff will:

a) Clear all systems holding student data: Client, Student Portal, and CRM
b) Clear all Clipboard data, see instructions – Staff Guidelines — Create shortcut to clear Clipboard
c) Delete any data from their desktop/shared drive/home drive folder of attached documents to the student

7. Guideline for Disclosure to Third Party – Parents/Partners/Family Members/Employer

Staff should not release information about a student to parents, partners, or other family members, unless the requestor is an **authorised agent** (see Agent Authorisation, section 9 below).

Staff may accept credit card payment of fees from a third party if the caller provides core information such as the student ID number and amount paid. Under no circumstances are staff to confirm or release any personal information held about individuals.

Payment of tuition fees by a third party does not entitle them to be given any personal information about the student. It is important to note that the student owns this information and has not authorised us to release it to their parents. This also applies when the third party is an employer.

8. Incapacitation or Death of Individuals

Callers with information on incapacitation or death of a student must be advised that they need to write to Student Registry, providing evidence of incapacitation or death of a student so that the appropriate action can be taken. Staff should not release information about a student to a third party unless the requestor is an authorised agent (see Agent Authorisation, section 9 below). Staff must follow the Deceased Student Procedure detailed in the internal Assyst FAQ system including internal notifications required to invoke Not for Outbounding and deceased status procedures.

9. Agent Authorisation

A student can nominate an agent to make inquiries on their behalf, by advising the University in writing using the Agent Authorisation form. A sample copy is attached in Appendix 2.

If a caller states that they are an approved agent for a student, staff must:

- Find the scanned copy of the Agent Authorisation form in SITS Client
- Confirm all of the key identifiers for the Agent against the authorisation form in SITS Client
  a) Agent full name (as shown on Agent Authorisation form)
  b) Agent date of birth (as shown on Agent Authorisation form)
  c) Current address/email address (as shown on Agent Authorisation form)
- Confirm all of all the key identifiers of the student with the Agent:
  a) Student full name
  b) Student date of birth
  c) Student current address or email address
- Proceed with the student look up when identification has been confirmed. Make the appropriate call history notes.

International Agents

Several international students will use the services of a Registered International Agent. You can view a list of Registered Agents on our website.

As part of the admission process, the international student along with the Agent will complete an Agent Authorisation Form and upload this with their Admission application.

If you receive a query from an Agent, please check the Agent Authorisation Form in the student portal under the Admission or Qualifications and courses tab under ACD Documents to confirm the agent's details

- Named Agent - we can only communicate with that one person, also ask for agency name and phone number and address from the form as well as standard verifiers for the student.

- Agency Listed only - we can communicate with anyone from the agency, check Agency and Phone number or Address, along with the student's standard verification details before releasing any information.

If you are unsure or unable to answer the Agents query, please contact the Admissions team, or forward to international@massey.ac.nz.

Do not release any information if there are unsatisfactory responses to the identifiers.

10. Power of Attorney

When a student gives someone (or a company) power of attorney, they give them the legal right to act on their behalf with one of two types of power of attorney, either an Ordinary Power of Attorney or an Enduring Power of Attorney. Students can provide a verified copy of a Power of Attorney in

lieu of an Agent Authorisation as this is a Legal Document and the same procedures above applied for Agent Authorisation are to be followed.

11. Guideline for Disclosure to Police

There is no legal requirement for staff to release student information when requested by the Police without further validation of the request.

The correct guideline when dealing with such a query is to:

- inform the requester to submit a document, such as search warrant or formal letter, with exact details of information requested and why; and
- direct the caller/requestor to the Governance and Assurance Office.

Note: if the police have no documentation but indicate the situation is urgent you can bypass step 1 and direct the caller/requestor through to the Governance and Assurance Office.

12. Guideline for Disclosure to Massey University Staff

In situations where a Massey University staff member is requesting student details, or changes to this information, **the Massey University Privacy Policy still applies**.

- Academic staff requesting information or changes are to be advised that they will need to contact their School/Departmental Secretary or School/Department Head.

- General staff, particularly library staff and Student Recruitment Advisors who are initiating a change to student details will need to either access this information themselves, contact their administrator, advise the student to call personally or to send the relevant paperwork to Student Registration.

13. Guideline for Refusing a Request for Information

In the event that the caller is a third party and information will be withheld, staff should inform the caller that they are withholding the information and the reason they are withholding the information.

Explain that:

- Release of information to an unauthorised third party is in breach of the Massey University Privacy Policy
- The student themselves may call to obtain or change their information or may authorise the third party to receive or change information provided that this is done in writing.
- If they are not satisfied with this response, they may redirect their request to the Privacy Officer at Massey (privacy.officer@massey.ac.nz).

14. Guideline for Handling Difficult Callers

Sometimes, where a refusal to release or change information has been made, a caller can become difficult. After the best possible effort has been made, the staff should refer the caller to their line manager who may in turn need to escalate the matter to Massey University Privacy Officer.

15. Notifying of a Data Breach at Massey

A privacy breach is where there has been any unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of personal information.

If you become aware of a privacy breach, please report it to you line manager straight away. Your line manager will follow the recommendations outlined in this Breach Notifications information sheet.

16. Privacy Officer

The Massey University Privacy Officer is:
Jodie Banner
Director Governance and Assurance
Massey University
Private Bag 11222
Manawatu Mail Centre
Palmerston North 4442
New Zealand

17. Request for Information under Official Information Act 1982

All requests for information under the Official Information Act 1982 should be directed to OIA@massey.ac.nz.

18. Privacy Complaints from Student/Staff

Please refer to your line manager.

19. Version Control

File Name: **Te Paepoto Privacy Guidelines**

Date	Status	Version	Updated by	Reason for Update
12/09/2006	Draft	1.0	Tina Hilliam	New guidelines document established. Sent to Anne Walker, Risk Manager and June Dallinger Director Human Resources for comment
15/09/2006	Final	1.1	Tina Hilliam	Document approved by Risk Manager and Director Human Resources. Issued to National Contact Centre staff.
02/10/2007	Review	1.2	Tina Hilliam	Annual review of guidelines. Document sent to Anne Walker, Risk Manager and June Dallinger Director Human Resources for comment
12/11/2007	Final	1.3	Tina Hilliam	Replaced Risk Manager with Registrar in Section 14 at request of Anne Walker. Document issued to staff.
5/09/2008	Review	1.4	Tina Hilliam	Updated section 4 to include clarification that personal information is stored in all media types and can be released instantaneously by staff once identifiers are checked. Updated Section 15 replaced June Dallinger with Michelle Ryan, Employment Relations Manager. Updated Appendix 1 & 2, MU Privacy Policy, Next Review: May 2010. Sent to Anne Walker, Risk Mgr and Michelle Ryan ER Mgr for review
18/09/08	Final	1.5	Tina Hilliam	Feedback received, document updated and issued to staff
20/11/09	Review	1.6	Tina Hilliam	Updated section 8 to include procedure for Agent Authorisation forms in exceptional or urgent circumstances. Updated Section 15 contact from Michelle Ryan to Angela van Welie. Full document sent for review to Anne Walker, Risk Mgr and Jenni Ward HR Adviser ER for review
30/11/09	Final	1.7	Tina Hilliam	Add new postal code format. Document approved. Issued to National Contact Centre staff.
16/11/11	Updated	1.8	Tina Rowland	Inserted Power of Attorney section, Updated Employment Relations Manager and AVC-UR Title, Updated Appendix 1-3 with latest versions. Distributed to Anne Walker, Risk Mgr, Fiona McMorran ER Mgr, Office of AVC-UR and all National Contact Centre staff.
19/09/13	Updated	1.9	Tina Rowland	Updated University postal address, updated HR to POD, NSATS/ Enrolment to Student Administration, updated Appendix 1-3 with latest versions. Biannual review of guidelines. Distributed to Anne Walker, Risk Mgr, Fiona McMorran ER Mgr, Office of AVC-UR and all National Contact Centre staff.
12/12/2013	Updated	2.0	Amanda Seymour-East	Replaced reference to the Privacy Act being quoted to callers. This was replaced with 'Massey University Privacy Policy'
28/10/2014	Updated	2.1	Amanda Seymour-East	Updated Appendix 1-3 with latest versions. Biannual review of guidelines.
29/01/2015	Updated	2.1	Melissa Eveleigh	Updated section 15 – Updated wording to clarify correct process.
22/009/2015	Updated	2.1	Melissa Eveleigh	Updated Privacy Officer from Anne Walker to Jodie Banner
4/10/2017	Updated	2.2	Amanda Mackrow	Updated Section 5. Guideline for Releasing Information to Individuals to include email as a form to identify a student Section 7. Incapacitation or Death of Individuals. Changed NOUT to not for outbounding Section 8. Changed SilentOne to Client Section 16. Changed the contacts to National Contact Centre Team Leaders
13/11/2018	Updated	2.3	Amanda Mackrow	Updated section 4: Added Social Media as a channel and added CRM as the system to record contact history. Added into section 5: How to label a document and how to clear data from systems and clipboard. Updated Appendix 1: Massey University Privacy Policy
7/12/2018	Updated	2.4	Frances Mullan/Jodie Banner	Removal of Procedures from Appendix 2 and renaming of Appendix 3 to 2 Removal of Procedures reference from Paragraph 2 Inclusion of GDPR references, rights and escalation processes Clarification of Agency relationships Extension of Access Request section to include rectification requests under Principle 7 Revision of Police Request and Escalation processes Addition of Privacy Officer escalation processes for request denials and difficult callers Addition of Info Request email to OIA section
14/05/2019	Updated	2.5	Amanda Mackrow	Updated the Privacy Office, page 5 to Jodie Banner

16/07/2019	Updated	2.6	Amanda Mackrow	Updated the document naming conventions in section 5.
8/06/2020	Updated	2.7	Amanda Mackrow	Updated National Contact Centre to Te Paepoto. Changed the email address for the privacy officer from inforequests@massey.ac.nz to OIA@massey.ac.nz.
9//09/2020	Updated	2.8	Amanda Mackrow	Updated the Office Information Act contact information in section 15. Updated section 8. Agent Authorisation, to make the identification process clearer.
3.11.2020	Updated	2.9	Amanda Mackrow	Corrected a link in section 5 to an FAQ on how to clear a clip board
14.12.2020	Updated	3.0	Amanda Mackrow	Slight update in the wording of section 5 to make the instruction of obtaining identification clearer.
17.05.2021	Updated	3.1	Amanda Mackrow	Added photo identification as appropriate for face to face assistance when completing identity checks.
13.08.2021	Updated	3.2	Amanda Mackrow	Updated Contact Relationship Manager to Customer Relationship Manager. Updated caller to customer in guideline 5. Added section 6. Receiving and uploading and sending documents Updated DIED to deceased in section 8. Updated Student Administration to Student Registry in section 9 and 12. Updated the Risk and Assurance Office to Risk Management in section 11. Updated his/her to themselves in section 13. Changed the reference from student to student
17.09.2021	Updated	3.3	Amanda Mackrow	Updated section 1 to refer to the Privacy Act 2020
12.05.2022	Updated	3.4	Amanda Mackrow	Updated the document name by removing Te Paepoto and adding Advising and Communication Removed Te Paepoto throughout the document. Update section 9 Agent Authorisation content due to a process change. Changed Team Leader to line manager throughout the document.
22.03.2023	Updated	3.5	Amanda Mackrow	Added a new section 15. Notifying of a Data Breach at Massey. Updated the word tauira to student until the university advises of the correct alternative.
3.04.2023	Updated	3.6	Amanda Mackrow	Removed link to International Agent FAQ and copied the actual information into this document. Replaced Risk and Assurance with Governance and Assurance

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Massey University Policy Guide

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.

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

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

MASSEY
UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

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

- Course of study and the fees for that course of study
- Changes to their course of study, if any
- Citizenship or residency status in New Zealand

- The progress of the student at Massey University (including the principal results achieved by the student) in his or her course of study.
- Particulars of any allowances, grants or other payments received by the student in respect of his or her course of study at the institution out of public money appropriated by Parliament.
- Such other information as must be kept so that Massey University can fulfill its obligations to provide the Secretary of Education with statistical information relating to students generally or to a particular class of student.
- Such other personal information relating to the student as may be reasonably required by the Chief Executive (as that term defined in Section 226A of the Education Act 1989) for the administration of the student loan scheme.

Prospective Students:

All personal information obtained by Massey University about a prospective student will be kept in a personal file for that prospective student.

If a prospective student does not become a student their personal file must be destroyed no later than five years after the last piece of information on the file was obtained.

Access to and correction of personal information:

Any staff member, student, prospective student or their agent may request access to all personal information about themselves held by Massey University other than evaluative material and other material that is subject to exception under the Information Privacy Principles in the Privacy Act 1993. If such a request is made then Massey University must provide the person making the request with access to that information, either by providing a copy or allowing viewing of the personal information, within a reasonable time.

Anyone is entitled to request correction of their own personal information other than evaluative material and other material that is subject to exception under the Information Privacy Principles in the Privacy Act 1993. Where such a request is made Massey University must decide whether or not to correct the personal information. Once it has decided Massey University must inform the staff member, student, prospective student or their agent of its decision. If Massey University decides not to correct the person's personal information then it must inform the person of their right to have their request and Massey University's refusal noted on their personal file. If a person decides to exercise this right then Massey University must note then the person's request and Massey University's refusal on the person's personal file.

Requests for Personal Information:

Massey University must not disclose personal information that it holds about any individual to any person, body or agency unless one of the exceptions in Principle 11 of the Information Privacy Principles applies.

Complaints:

Any Massey University staff member, student or prospective student may complain to Massey University that there has been a breach of the Privacy Information Principles in relation to themselves. Where a complaint is received under this Clause it will be dealt with through the privacy complaints procedure set out in Appendix 2.

RELATED PROCEDURES / DOCUMENTS

Privacy Policy & Privacy Management Framework
Privacy Impact Assessment Toolkit
Records Management Policy and Procedures

DOCUMENT MANAGEMENT

Prepared by:	Risk Manager
Authorised by:	AVC Operations, International and University Registrar
Approved by:	n/a
Date issued:	May 2006
Last review:	July 2014
Next review:	July 2017

APPENDIX 1:

INFORMATION PRIVACY PRINCIPLES AS OUTLINED IN THE PRIVACY ACT 1993

PRINCIPLE 1

Purpose of collection of personal information
Personal Information shall not be collected by any agency unless –

(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and
(b) The collection of the information is necessary for that purpose.

PRINCIPLE 2

Source of personal information

1. Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

2. It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds, -
   (a) That the information is publicly available information; or
   (b) That the individual concerned authorises collection of the information form someone else; or
   (c) That non-compliance would not prejudice the interests of the individual concerned; or
   (d) That non-compliance is necessary –
      i. To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences; or
      ii. For the enforcement of a law imposing a pecuniary penalty; or
      iii. For the protection of the public revenue or
      iv. For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or
   (e) That compliance would prejudice the purpose of the collection; or
   (f) That compliance is not reasonably practicable in the circumstances of the particular case; or
   (g) That the information –
      i. Will not be used in a form in which the individual concerned is identified; or
      ii. Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
   (h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.

PRINCIPLE 3

Collection of information from subject

1. Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of –
   (a) The fact that the information is being collected; and
   (b) The purpose for which the information is being collected; and
   (c) The intended recipients of the information; and
   (d) The name and address of –

i. The agency that is collecting the information; and
ii. The agency that will hold the information; and

(e) If the collection of the information is authorised or required by or under law, -
i. The particular law by or under which the collection of the information is so authorised or required; and
ii. Whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) The rights of access to, and correction of, personal information provided by these principles.

2. The steps referred to in subclause (1) of this principle shall be taken before the information is collected, or, if that is not practicable, as soon as practicable after the information is collected.

3. An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

4. It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,
(a) That non-compliance is authorised by the individual concerned; or
(b) That non-compliance would not prejudice the interests of the individual concerned; or
(c) That non-compliance is necessary –
i. To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences, or
ii. For the enforcement of a law imposing a pecuniary penalty; or
iii. For the protection of the public revenue; or
iv. For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or
(d) That compliance would prejudice the purposes of the collection; or
(e) That compliance is not reasonably practicable in the circumstances of the particular case; or
(f) That the information –
i. Will not be used in a form in which the individual concerned is identified; or
ii. Will not be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

PRINCIPLE 4

Manner of collection of personal information

Personal Information shall not be collected by an agency –
(a) By unlawful means; or
(b) By means that, in the circumstances of the case, -
i. Are unfair; or
ii. Intrude to an unreasonable extent upon the personal affairs of the individual concerned.

PRINCIPLE 5

Storage and security of personal information

An agency that holds personal information shall ensure –

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against –
   i. Loss; and
   ii. Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
   iii. Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

PRINCIPLE 6

Access to personal information

1. Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled –
   (a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and
   (b) To have access to that information

2. Where, in accordance with subclause (1) (b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

3. The application of this principle is subject to the provisions of Parts IV and V of this Act.

PRINCIPLE 7

Correction of Personal Information

1. Where an agency holds personal information, the individual concerned shall be entitled -
   (a) To request correction of the information; and
   (b) To request that there be attached to the information a statement of the correction sought but not made.

2. An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete and not misleading.

3. Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

4. Where the agency has taken steps under sub clause (2) or sub clause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

5. Where an agency receives a request made pursuant to sub clause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

PRINCIPLE 8

Accuracy, etc, of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant and not misleading.

PRINCIPLE 9

Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes of which the information may lawfully be used.

PRINCIPLE 10

Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds, -

(a) That the source of the information is a publicly available publication; or
(b) That the use of the information for that other purpose is authorised by the individual concerned; or
(c) That non-compliance is necessary –
    i. To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences; or
    ii. For the enforcement of a law imposing pecuniary penalty; or
    iii. For the protection of the public revenue; or
    iv. For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or
(d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to –
    i. Public health or public safety; or
    ii. The life or health of the individual concerned or another individual; or
(e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or
(f) That the information –
    i. Is used in a form in which the individual concerned is not identified; or
    ii. Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(g) That the use of the information is in accordance with an authority granted under section 54 of this Act.

PRINCIPLE 11

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds, -

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
(b) That the source of the information is a publicly available publication; or
(c) That the disclosure of the individual concerned; or
(d) That the disclosure is authorised by the individual concerned; or
(e) That non-compliance is necessary –
    i. To avoid prejudice to the maintenance of the law by any public sector agency; including the prevention, detection, investigation, prosecution and punishment of offences; or
    ii. For the enforcement of a law imposing a pecuniary penalty; or
    iii. For the protection of the public revenue; or
    iv. For the conduct of proceedings before any court or (tribunal) (being proceedings that have been commenced or are reasonably in contemplation); or
(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to –
    i. Public health or public safety; or
    ii. The life or health of the individual concerned or another individual; or
(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or
(h) That the information –
    i. Is to be used in a form in which the individual concerned is not identified; or
    ii. Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

PRINCIPLE 12

Unique identifiers

1. An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

2. An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of (section OD 7 of the Income Tax Act 1994).

3. An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

4. An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

APPENDIX 2:

COMPLAINTS PROCEDURE

1. If a complaint is made whether orally or in writing to a staff member by any individual regarding their own personal information then the staff member shall endeavor to resolve the complaint directly with the person concerned.

2. If the complaint is not resolved then the staff member shall refer the complainant to the University's Privacy Officer.

3. On receipt of a complaint, the Privacy Officer shall ascertain the nature of the complaint and endeavor to bring about a resolution to the complaint.

4. This procedure does not affect any rights the complainant might have under the Privacy Act 1993 or the University in relation to the Student Contract (see Massey University Calendar) or Grievance procedures.

APPENDIX 2:

COMPLAINTS PROCEDURE

1. If a complaint is made whether orally or in writing to a staff member by any individual regarding their own personal information then the staff member shall endeavor to resolve the complaint directly with the person concerned.

2. If the complaint is not resolved then the staff member shall refer the complainant to the University's Privacy Officer.

3. On receipt of a complaint, the Privacy Officer shall ascertain the nature of the complaint and endeavor to bring about a resolution to the complaint.

4. This procedure does not affect any rights the complainant might have under the Privacy Act 1993 or the University in relation to the Student Contract (see Massey University Calendar) or Grievance procedures.

APPENDIX 2: Agent Authorisation Form

MASSEY UNIVERSITY
UNIVERSITY OF NEW ZEALAND

AGENT AUTHORISATION FORM

Student's details

MASSEY STUDENT ID NUMBER (IF KNOWN)

NAME

Surname: _____

First name(s): _____

DATE OF BIRTH

Day | Month | Year

ADDRESS

Address: _____

Suburb: _____

Town/city: _____

Postcode: _____ Country: _____

E-mail: _____

Phone: _____

Agent's details

NAME

Surname: _____

First name(s): _____

DATE OF BIRTH

Day | Month | Year

ADDRESS

Address: _____

Suburb: _____

Town/city: _____

Postcode: _____ Country: _____

Phone (day): _____

Email: _____

Declaration

I authorise my Agent to have access to my Massey University file, to change any details, request any information and speak on my behalf. I authorise my Agent to receive access to such information either in person, through the phone, or through electronic or other means:

from: Day | Month | Year

to: Day | Month | Year

or have access from:

Day | Month | Year

until I notify otherwise.

Signed (by student – verified copy of signature)

_____

Date Day | Month | Year

Please send completed form to:
Academic Support
Massey University
Private Bag 11222
Palmerston North 4442
NEW ZEALAND