Privacy Management Plan

Contents

1. Introduction

1.1 Purpose

The purpose of this Privacy Management Plan (the Plan) is to explain how Macquarie University (the University) manages Personal and Health Information in accordance with the University's Privacy Policy and the following applicable privacy laws:

- Privacy and Personal Information Protection Act 1998 (NSW) (the PPIP Act)
- Health Records and Information Privacy Act 2002 (NSW) (the HRIP Act)

In particular, the Plan addresses the Information Protection Principles (the IPPs) and the Health Privacy Principles (the HPPs) contained within the above Acts. These privacy principles regulate Collection, storage, access and correction, security, Use and Disclosure of Personal Information in NSW. Section 33 of the PPIP Act requires agencies, including the University, to have a Privacy Management Plan.

The Plan provides details on who to contact with any questions about the Collection and storage of Personal or Health Information, how to access or amend Personal Information and how to make a complaint if you believe that the University may have breached the PPIP or HRIP Acts.

This Plan is one of the key tools used to inform University Staff and Affiliates about how to handle Personal and Health Information and raise awareness of the University's privacy obligations.

1.2 What the Plan covers

The Plan meets the requirements of s33(2) of the PPIP Act by:

- providing information about how the University devises policies and practices in accordance with the State's records, information access and privacy acts;
- explaining how the University disseminates these policies and practices and trains staff in their use;
- detailing the University's internal review procedures;
- outlining the procedures and practices used by the University to ensure compliance with the obligations and responsibilities for the mandatory notification of data breach scheme; and
- documenting any other matters deemed relevant by the University in relation to the privacy and protection of Personal Information held by the University.

1.3 Scope

This Plan covers the activities of Staff, Students and Affiliates of the University. The Plan does not apply to the University's Controlled Entities. Controlled Entities are required to develop privacy policies and plans consistent with their obligations under relevant legislation.

1.4 Definitions

Refer to Appendix A for definitions.

1.5 Review cycle

This Plan will be reviewed on an annual basis and updated where required.

2. The University's functions and activities

2.1 Object and functions

The University collects, retains, uses and discloses Personal Information in the course of meeting its object and exercising its functions as set out in the *Macquarie University Act 1989* (NSW). The object of the University is the "promotion within the limits of the University's resources, of scholarship, research, free inquiry, the interaction of research and teaching, and academic excellence."

The University has the following principal functions for the promotion of its object—

(a) the provision of facilities for education and research of university standard,
(b) the encouragement of the dissemination, advancement, development and application of knowledge informed by free inquiry,
(c) the provision of courses of study or instruction across a range of fields, and the carrying out of research, to meet the needs of the community,
(d) the participation in public discourse,
(e) the conferring of degrees, including those of Bachelor, Master and Doctor, and the awarding of diplomas, certificates and other awards,
(f) the provision of teaching and learning that engage with advanced knowledge and inquiry,
(g) the development of governance, procedural rules, admission policies, financial arrangements and quality assurance processes that are underpinned by the values and goals referred to in the functions set out in this subsection, and that are sufficient to ensure the integrity of the University's academic programs.

The University has other functions as follows—

(a) the University may exercise commercial functions comprising the commercial exploitation or development, for the University's benefit, of any facility, resource or property of the University or in which the University has a right or interest (including, for example, study, research, knowledge and intellectual property and the practical application of study, research, knowledge and intellectual property), whether alone or with others,
(a1) without limiting paragraph (a), the University may generate revenue for the purpose of funding the promotion of its object and the carrying out of its principal functions,
(b) the University may develop and provide cultural, sporting, professional, technical and vocational services to the community,

(c) the University has such general and ancillary functions as may be necessary or convenient for enabling or assisting the University to promote the object and interests of the University, or as may complement or be incidental to the promotion of the object and interests of the University,
(d) the University has such other functions as are conferred or imposed on it by or under this or any other Act.

The functions of the University may be exercised within or outside the State, including outside Australia.

2.2 University records containing Personal Information

The University collects Personal Information to support its functions and activities related to learning and teaching, research, Student administration, Student services, complaints and conduct, recruitment and employment, health and well-being, employment and relationships with external parties for commercial, philanthropic and marketing purposes.

In exercising its functions (and related activities), the following records of the University will be collected and contain Personal Information. Note this list is not exhaustive.

	Students	Staff	External
Type	- Personal identifiers (e.g. names, student identification numbers, address, contact details); - Digital photos for student identification cards; - Financial information (e.g. tax file numbers, HECS information, information relating to student loans); - Assessment information (including examiners' reports, practicum assessments, academic results); and - Information and communication technologies records such as cookies, websites etc.	- Personal identifiers (e.g. names, staff identification numbers, address, contact details); - Digital photos for staff identification cards; - Financial information (e.g. tax file numbers, banking details, remuneration details, superannuation details); and - Previous employment details	- Personal identifiers (e.g. names, contact details) of individuals associated with the University such as members of governance bodies/committees, benefactors, sponsors, consultants, contractors, suppliers, users of the University's facilities etc.; - Financial information (e.g. banking details of contractors, consultants, suppliers); - Some records of the University's governance bodies (particularly Council, and Academic Senate and its subcommittees) may refer to Personal Information relating to external persons; and - Alumni and donor records

	As a health service provider	As a public educational institution	As an employer
Type	- Medical records of patients receiving health services from any of the Clinics, counselling services etc.	- Student welfare information (e.g. health and medical information, disability and equity information); and - Research involving the use of Health Information	- Staff welfare information (e.g. health and medical information related to employment including sick leave documentation; Workers Compensation and Occupational Health and Safety records and information; disability and equity information)

The University's research and teaching activities can involve the Collection of data from individuals who are both internal and external to the University. Such data may include Personal or Health Information held by the University or individual researchers. Human-based research projects require prior approval by the University's Human Ethics Research Committee (HREC), and as part of this process, consent is normally obtained in respect of the Collection, Use and Disclosure of Personal or Health Information for research purposes.

Consent for research purposes may not always be required in certain situations (see section 17.2 of this Plan).

2.3 Privacy-related policies, procedures and statements

- Privacy Policy
- Data Breach Policy
- Collection Notices
- Cyber Security Policy
- Computer and Network Security Procedure
- Information Classification and Handling Procedure
- Records and Information Management Policy
- Access and Security Procedure
- Retention and Disposal Procedure
- Right to Information at Macquarie
- Release of Student Information Procedure
- Research Data Management Policy
- Research Data Management Procedure; and
- Research Data Sensitivity, Security and Storage Guideline

2.4 Training and awareness

All Staff members and Affiliates who handle Personal Information must be familiar with this Plan, the Privacy Policy and other applicable University policies and privacy Collection Notices.

All staff must complete the online training module – *Privacy in Practice* – available on Workday and repeat this training every two years.

A customised privacy training/workshop can be provided by the Privacy Manager on request.

3. Roles and responsibilities

Privacy function accountabilities	Privacy governance structure
· Manage the overall privacy framework including distributing procedures and guidelines to support compliance with the Privacy Policy and Privacy Management Plan; · Provide advice and support for privacy related queries and where matters are escalated (e.g. high risk projects or initiatives, data subject requests); · Ensure delivery of training (University wide and targeted) and awareness activities; · Update the University wide framework when new external and internal privacy requirements have been identified; · Support the incident management framework where it relates to privacy or data breaches; · Handling privacy complaints and completing internal reviews; and · Liaise with the relevant regulatory authorities for matters relating to privacy and personal information.	**Executive Group Members** · Ensuring that University-wide procedures that support the Privacy Policy and Privacy Management Plan are applied in the management of personal and health information within their respective portfolios; and · Implementing local procedures to ensure that personal and health information that is held within their portfolio is managed in accordance with University policies and procedures and the relevant privacy legislation. **Information Technology and Cyber Security** · Establishing an IT control environment to protect personal information from loss, unauthorised access, use, modification or disclosure; · Identifying, monitoring and responding to data breaches; and · Ensuring third party IT environments adhere to the University's security requirements where personal information will be held, accessed or stored. **Implementation, project and business owners** · Ensuring privacy impact assessments on new and/or high risk activities under their stewardship are undertaken; · Conducting data privacy and security assessments on third party IT architecture and solutions; and · Ensuring the local procedures to manage personal information are operating as intended e.g. limiting and securing access to personal information to only those who require it and reviewing access periodically to ensure it remains appropriate. **All staff, students and affiliates** · Being aware of their privacy obligations and responsibilities; · For staff, completing any required privacy training with team managers to follow up incomplete training; · Handling personal information in accordance with the Privacy Policy, the Privacy Management Plan and other related policies and procedures; and · Reporting any data breaches or breaches of privacy.

4. Privacy by Design

Across all stages of the Personal Information lifecycle, the following principles must underpin the University's approach to the management of Personal Information (as adapted from the NSW Information and Privacy Commission's Privacy by Design Fact Sheet):

- take a proactive approach, anticipating risks and preventing privacy-invasive events before they occur;
- automatically protect Personal Information in IT systems and University practices as the default;
- embed privacy into the design of all systems, services and University practices, ensuring that privacy becomes one of the core principles of any system or service;
- incorporate all legitimate interests and objectives with a balanced approach to competing priorities (a "win-win" manner), avoiding unnecessary trade-offs, such as between privacy and security;
- put in place strong security measures throughout the Personal Information lifecycle, processing Personal Information securely, documenting maximum period of retention, and destroying Personal Information securely once the information is no longer required;
- ensure that whatever practice or technology used by the University to handle Personal Information operates according to the stated promises and objectives and is independently verifiable;
- actively seek methods to be transparent and make information available to individuals whose Personal Information is held by the University that is clear, easy to understand and accessible;
- keep the interests of individuals paramount in the design and implementation of any system or service, by offering strong privacy defaults and user-friendly options, and ensuring appropriate notice is given; and
- ensure that any system that holds Personal Information will have a Privacy Impact Assessment (PIA) undertaken and reviewed by the University's Privacy Officer before the system design is finalised. Refer to the PIA Template and Guidance available on Policy Central.

5. Collecting Personal and Health Information

The following principles must be adhered to when collecting Personal Information:

- the University can only collect Personal or Health Information for a lawful purpose, directly related to our functions and activities;
- at the time of Collection, or as soon as possible afterwards, a Collection Notice must be provided to individuals to whom the Personal Information relates. The purpose of the Collection should align with the University's Privacy Collection Notices. There may be instances where the Collection Notices do not adequately cover the circumstances, and a tailored collection notice will need to be prepared;
- Collection notices must inform individuals:

i) that their information is being collected;
ii) the purposes for which their information is being collected;
iii) the intended recipients of this information;
iv) whether the supply of the information is required by law or is voluntary, and any consequences for individuals of not providing the information;
v) the existence of any right to access, and correct, their information; and
vi) the name and address of the University.

- minimise the amount of Personal Information that is processed, only collecting information that it necessary for the University's purposes;
- Collection must not be excessive and should not unreasonably intrude into the personal affairs of the individuals concerned;
- where deemed necessary, undertake a Privacy Impact Assessment (PIA) prior to collecting Personal Information, in accordance with the PIA Guidance Note; and
- collect the Personal or Health Information directly from the individual to whom it relates, unless the individual has authorised Collection from someone else or a relevant exemption in the Acts apply.

There may be instances where the University collects Personal Information from third parties, including where:

- UAC applicants authorise the University to collect their application information for the purposes of assessment for an offer of a place in a course offered by the University;
- Students/Staff can authorise the University to collect Health Information from their medical or health practitioners; and/or
- parents of children under 16 can provide this information on behalf of their children.

6. Retention and security of Personal Information

6.1 General requirements

The University must ensure that Personal Information held:

- is kept for no longer than is necessary for the purposes for which the information can be lawfully used;
- is disposed of securely and in accordance with any requirements for the retention and disposal of Personal Information;
- is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or Disclosure, and against all other misuse; and
- that, if it is necessary for the information to be given to a person in connection with the provision of a service to the University, everything reasonably within the power of the University is done to prevent unauthorised use or Disclosure of the information.

The University must undertake the following to ensure these security requirements are met:

- all storage systems (both physical and electronic) must be assessed

periodically to ensure they have the appropriate safeguards in place to protect Personal and Health Information, noting that the safeguards may need to vary depending on the sensitivity of the information;
- when Personal and Health Information is stored, processed or handled by third parties on behalf of the University, they must be bound by a legally binding agreement that requires the third party to comply with the University's retention and security requirements and the applicable legislation;
- access must be restricted to only those Staff that require access to the information to perform their legitimate work functions; and
- access rights must be periodically reviewed (at least quarterly) to ensure that it remains appropriate.

6.2 Third party service providers

The University must have the following measures in place where a third party will handle the Personal Information held by the University:

- contracts with third party providers must include appropriate standards for data protection and require compliance with the relevant privacy principles; and
- where the University intends to disclose Personal or Health Information to a third party service provider outside of NSW or to a Commonwealth agency, the University takes reasonable steps to ensure that the information it has disclosed will not be held, used or disclosed by the recipient inconsistently with the IPPs / HPPs. It does this by:
    - including contractual protections requiring the recipient to comply with the IPPs / HPPs and the Privacy Commissioner's guidance on transborder disclosures;
    - making an assessment to determine that the privacy protections operating in the destination jurisdiction are substantially similar to those in NSW;
    - conducting audits over the service providers' IT systems before the contract is entered into and during the term of the contract;
    - minimising the data shared with the third party to only the Personal Information that is necessary for the performance of the contract; and
    - ensuring that third party access is limited to employees on a 'needs-to-know' basis for the purposes of the contract and are aware of their privacy obligations.

6.3 Retention and disposal of Personal Information

Personal Information must be retained in accordance with the University's Records and Information Management Policy and any statutory retention obligations, such as the State Records Act.

The University has a Records and Retention Guide that provides guidance on retention periods for commonly held University records, which may include Personal Information. The advice of the Archives and Records team should be obtained in determining retention periods for Personal Information, as well as the method and timing of disposal.

Following the retention period, Personal and Health Information must be destroyed

securely and without delay.

7. Ensuring the accuracy of Personal Information

All Personal and Health Information should be verified at the time of Collection to ensure its accuracy.

The University must:

- verify external documents with the issuer, where applicable. For example, academic transcripts with other institutions provided for admission purposes must be verified with the institution that issued the transcript, with the individuals' consent; and
- ensure individuals are aware of how to update their Personal Information to maintain accurate records.

8. Use of Personal Information

8.1 General requirements

Access to University systems is not immediately granted to all staff members by virtue of being an employee of the University. Staff should only have access to the University's systems where there is a legitimate work purpose. Role-based user access levels that restrict the types and amount of Personal Information that staff can access, and use should also be utilised to manage the use of Personal Information for legitimate purposes relating to the functions of the University.

8.2 Use of Student Personal Information

Personal Information of Students must only be used for the purposes outlined in the Privacy Statement/Student Collection Notice. Students acknowledge this statement at enrolment and when providing Personal Information when accessing services supporting their enrolment, e.g. on Service Connect. The University must obtain the Student's consent prior to using their Personal Information for any other purpose, except where authorised or required by law. Students may withdraw their consent in writing at any time.

8.3 Use of Staff Personal Information

Personal Information of Staff must only be used for the purposes outlined in the Privacy Statement/Staff Collection Notice. Staff acknowledge this statement when they accept their offer of employment. The University must obtain the Staff member's consent prior to using their Personal Information for any other purpose, except where authorised or required by law. Staff may withdraw their consent in writing at any time.

8.4 Use of alumni Personal Information

Personal Information of alumni must only be used for the purposes outlined in the Alumni Collection Notice. The University must obtain the alumni's consent prior to

using their Personal Information for any other purpose, except where authorised or required by law. Alumni may withdraw their consent in writing at any time.

9. Disclosure of Personal Information

9.1 General requirements

Under the PPIP Act, the University must not disclose Personal Information unless:

- the Disclosure is directly related to the purpose for which the information was collected, and the University has no reason to believe that the individual concerned would object to the Disclosure;
- the individual concerned is reasonably likely to have been aware, or has been made aware through the University's Collection notices, that information of that kind is usually disclosed to another person or body; and/or
- the University believes on reasonable grounds that the Disclosure is necessary to prevent or lessen a serious or imminent threat to the life or health of the individual concerned or another person.

The University's Privacy Statement also sets out circumstances in which Personal Information collected by the University may be disclosed.

The University will only disclose Personal Information outside the organisation where the above apply, or where authorised or required by law. The University will obtain the consent of the individual concerned prior to disclosing their Personal Information for any other purpose.

9.2 Disclosure of Health Information

Under the HRIP Act, the University can disclose an individuals' Health Information for a secondary purpose if:

- the individual has consented; or
- the secondary purpose is directly related to the primary purpose for which the information was collected, and the individual would reasonably expect the University to disclose that information for a secondary purpose; or
- where an individual has been made aware, or is likely to be aware, that information of that kind is usually disclosed to the body or person that the University wishes to disclose the information to; or
- the University believes, on reasonable grounds, that the Disclosure is necessary to prevent or lessen a serious and imminent threat to the life, health or safety of a person or a serious threat to public health or safety; or
- the University has reasonable grounds to suspect an unlawful activity has been or may be engaged in; or
- necessary for the exercise of law enforcement functions by law enforcement agencies; or
- necessary for the exercise of complaint handling functions or investigative functions by investigative agencies; or
- the Disclosure is permitted by a Public Interest Direction made by the NSW Privacy Commissioner (see section 17.1 of this Plan).

10. Sensitive Personal Information

Sensitive Personal Information includes information which relates to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual activities. It also includes Health Information about an individual (as defined by the HRIP Act), genetic information and biometric information.

Disclosure of Sensitive Information can only be made with the consent of the individual concerned.

The University only uses health records linkage systems (such as My Health Record) when individuals have expressly consented to their information being included on such a system, unless an exemption applies.

11. Health records linkage systems

A "health records linkage system" means a computerised system designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records.

The University only uses health records linkage systems (such as My Health Record) when individuals have expressly consented to their information being included on such a system, unless an exemption applies.

12. Individual identifiers

The University assigns unique identifiers for the purpose of patient identification. This is necessary in the University's capacity as a Health Care Service Provider for the identification of patients and their treatments. It is acknowledged that these identifiers are classified as Health Information and are subject to the HRIP Act and protected as such. The University also assigns a unique identifier to all Students and Staff (their OneID).

13. Anonymity

Wherever it is lawful and practicable, the University will provide people the opportunity to remain anonymous when entering into transactions with, or receiving health services from, the University.

However, in the context of providing health services it is impracticable to transact with an individual anonymously due to the type of information required from an individual, such as:

- personal contact details;
- Medicare details and private health insurance information being required to complete the transaction;
- previous medical history, referrals etc.;

- ongoing health care requiring follow-up; and
- bank account/credit card details.

There may be some instances where an individual can remain anonymous when engaging with the University. These include:

- reporting a safety risk, hazard, near-miss incident or injury through the Risk and Safety Reporting system;
- providing anonymous feedback or completing surveys;
- participating in some research projects; and/or
- reporting serious wrongdoing under the Public Interest Disclosure Policy.

14. Accessing Personal Information

Requests for access should follow the Request for Information process. Individuals can also contact the Privacy Officer with requests for access to their Personal Information. The University will allow any individual to access the information held about them in accordance with the PPIP Act and HRIP Act, in most cases at no cost and through an informal request process. Applications for access will be processed in a timely fashion.

There may be some instances where these requests may be referred to action under the Government Information (Public Access) Act (GIPA Act). This includes where the information contains the Personal Information of another individual. Applications are therefore subject to the public interest considerations against Disclosure in the GIPA Act which will override the access rights provided by the PPIP Act and HRIP Act.

Access to information about a third party is not accessible under the Privacy Acts.

The Access to Personal Information Guidance Note provides further information.

14.1 Access by Students

Students are able to access information relating to their enrolment at the University through eStudent or the Service Connect Portal.

14.2 Access by Staff

Staff are able to access their Personal Information relating to their employment through the Workday portal.

14.3 Applying for Personal or non-personal Information under the GIPA Act

Members of the public and Students or Staff may apply under the GIPA Act for access to any information held by the University, including information about themselves. There is a statutory application fee of $30 plus processing charges may also apply. Further information and an application form are available on the University's Right to Information (GIPA) website.

15. Amending Personal Information

15.1 Amendment by Students

Students are able to amend some of their Personal Information through eStudent and the Service Connect portal. Changes to official information (i.e. first name, last name, date of birth) require a certified copy of official documentation. Refer to the Change of personal details webpage for more information.

15.2 Amendment by Staff

Staff are able to amend some of their Personal Information through the Workday Portal.

15.3 Amendment by alumni

Alumni are able to update their personal contact details through the Alumni website.

15.4 Other options to amend Personal Information

An individual who wishes to make amendments to Personal Information, which is not covered by the processes above, may contact the Privacy Officer.

The University may agree to amend the information and if so, will inform the individual accordingly. If the University decides not to amend the information, reasons will be provided to the applicant along with information regarding their rights to seek an internal review – refer to section 19.

16. Public Registers

A public register is an official list of names, events and transactions. Under law, it is required to be available to the public.

The University maintains a Graduate Register that can be accessed by members of the public, The Register allows searches of graduate' names and provides their awards conferred and conferral dates. Some information is also publicly available through University publications, such as Staff details, and graduation records.

17. Exemptions from IPPs/HPPs

17.1 Overview

Under s41 of the PPIP Act and s62 of the HRIP Act, the Privacy Commissioner may make a direction or modify the requirement for an agency to comply with an IPP or a Code of Practice. The Information and Privacy Commission NSW publishes current Codes of Practice that have been approved and gazetted and can be found here. The University does not currently have an approved Code of Practice.

17.2 Research exemptions

The University may collect, use and disclose Personal Information for research purposes without obtaining an individual's consent provided it complies with all the criteria set out in section 27B of the PPIP Act, any Statutory Guidelines issued by the Privacy Commissioner and approval is obtained from the University's Human Research Ethics Committee.

The University may collect, use and disclose Health Information for research purposes without obtaining an individual's consent provided it complies with all the conditions set out in HPP10(1)(f) and HPP11 (1)(f) of the HRIP Act, any Statutory Guidelines issued by the Privacy Commissioner and obtains approval of the University's Human Research Ethics Committee.

18. Mandatory Notification of Data Breach Scheme

18.1 General requirements

The Mandatory Notification of Data Breach Scheme (MNDB Scheme) requires the University, in the event of a suspected data breach, to contain the breach and assess the likely severity of harm to the impacted individuals. The assessment must be completed within 30 days of the University becoming aware of the breach.

Where the breach is likely to result in serious harm, as defined in the Privacy Acts, to an individual (an eligible data breach), the University is required to notify the NSW Information and Privacy Commissioner as well as the impacted individuals. Where it is not practicable to notify each individual, a public notification will be issued.

All suspected and actual data breaches must be handled in accordance with the Data Breach Policy.

19. Complaints and internal reviews

19.1 Informal process

Individuals are encouraged to resolve their privacy complaint informally where possible. If there are any concerns with how Personal Information has been handled, the area that holds this information can be contacted directly, or individuals can contact the Privacy Officer for assistance or guidance.

19.2 Application for internal review under the PPIP Act

The PPIP Act also allows individual who are "aggrieved" by the conduct of the University to make an application for internal review.

An application for internal review can only be made where it is alleged that the University has:

- breached any of the IPPs or HPPs; or

- breached any code made under the PPIP Act applying to the University; or
- disclosed Personal Information kept in a public register of the University.

An application for internal review must:

- be in writing;
- be addressed to the University;
- be lodged within 6 months from the time the applicant became aware of the conduct;
- comply with any other requirements as prescribed by the regulations.

Individuals may use the Application for internal review form which should be sent to the Privacy Officer.

If the review is not completed within 60 days from the date the application was received or the complainant is dissatisfied with the University's findings, then the complainant has 28 days to make an application under section 55 to the NSW Civil and Administrative Tribunal (NCAT) for a review of the conduct or decision complained about.

19.3 The role of the Privacy Commissioner in internal reviews

The NSW Privacy Commissioner has an oversight role in the internal review process and may make submissions on internal reviews.

The University is required under the Privacy legislation to notify the Privacy Commissioner regarding the following:

- formal complaints received;
- progress on internal reviews being undertaken; and
- findings of the reviews undertaken and the action proposed to be taken by the University.

The Privacy Commissioner is entitled to make submissions to the University with respect to the findings of the internal review and may at the request of the University undertake the internal review on behalf of the University.

19.4 Making a complaint to the NSW Privacy Commissioner

A person aggrieved by the conduct of the University may complain directly to the NSW Privacy Commissioner, not as an external review mechanism, but as a complaint.

In this instance, the Privacy Commissioner may conduct a preliminary assessment of a complaint before deciding whether to deal with the complaint.

20. Other applicable laws

20.1 Commonwealth Privacy Act

The University is not required to comply with the Australian Privacy Principles in the

Privacy Act 1988 (Cth) (Privacy Act) as it is not an 'organisation' within the meaning of the Act.

However, the University is a 'file number recipient' for the purposes of the Privacy Act because it holds records of employees and Students which contain tax file number information. As such, the University must comply with any rules relating to tax file number information issued under section 17 of the Privacy Act.

The University's Controlled Entities that are considered "organisations" are subject to the Privacy Act.

The University must ensure that any information provided by the University to another organisation is protected to the same standards that the University applies to the information it holds. Therefore, in any dealings between the University and its Controlled Entities in relation to Personal and Health Information, the standards applicable to the University (i.e. under the PPIP Act and HRIP Act) must be applied in addition to the requirements under the Privacy Act.

20.2 Government Information (Public Access) Act 2009 (GIPA)

The operation of the Government Information (Public Access) Act 2009 is not affected by the operation of the PPIP Act and the HRIP Act.

Note that GIPA provides access to various documents held by the University to any person subject to the operation of various exemptions in that Act. Under the PPIP Act and the HRIP Act, access to information is provided only to the person to whom the information relates.

20.3 State Records Act NSW 1998

The University is required to comply with the NSW State Records Act and associated Standard on Records Management issued by the State Records NSW. The provisions within the State Records Act provide overall guidance on the practical requirements for effective records and information management including retention periods and disposal of records and should be considered in conjunction with the Privacy Acts.

20.4 General Data Protection Regulation (EU2017/679)

The University is required to comply with the General Data Protection Regulation (GDPR) where it meets specific criteria such as collecting and/or processing personal data of European Union (EU) residents or providing goods and services to EU residents.

Personal data is defined within GDPR as any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mantal, economic, cultural or social identify of that natural person.

‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, Use, Disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Some specific circumstances where GDPR will apply to the University include, but are not limited to:

- the University processes data that belongs to Students or Staff who are EU residents;
- the University offers programs, courses, or unit of studies to Students who are EU residents; and
- the University enters a contract with a third party that requires it to comply with the provisions of GDPR;

GDPR outlines seven protection and accountability principles that the University is required to comply with when processing data of EU residents. While many of these principles are fundamentally similar to the IPPs and HPPs, they do impose stricter conditions on the management of Personal Information.

As a data controller, the University is required to:

- implement a ‘privacy by design and default’ approach to show that the University has integrated effective measures to protect personal data into its processing activities;
- maintain records of processing activities under its responsibility;
- undertake a data protection impact assessment (DPIA) before commencing data processing of EU individuals where the processing is likely to result in a high risk to individuals’ rights and freedoms;
- consult with a relevant supervisory authority before processing begins if the DPIA indicates that processing operations, in the absence of mitigation measures, pose a high risk to the rights and freedoms of EU individuals; and
- advise a relevant supervisory authority within seventy-two (72) hours of becoming aware of a data breach (unless it is unlikely to result in a high risk to the rights and freedoms of individuals).

The individual ‘data subject’ has various privacy rights under the GDPR, some of which do not have a direct equivalent in the NSW privacy legislation. There must be a clear legal basis for processing of personal data, and consent to any data processing must be freely given, specific, informed and unambiguous. Along with access and amendment rights, individuals may have the right to:

- object to or restrict the processing of their data;
- data portability e.g. to have data transferred to another organisation; and
- be forgotten, where data subjects can request the deletion of their information that the University holds.

Any individual who is an EU resident and wishes to exercise their privacy rights under the GDPR can contact the Privacy Officer.

21. Offences

Part 8 of the PPIP Act and HRIP Act details offences for certain conduct. A table detailing the relevant penalties and associated provision has been provided below.

Offence	Maximum penalty	Legislative provision
It is a criminal offence for a public sector official to corruptly disclose and use Personal or Health Information	• Fine of up to 100 penalty units ($11,000), or • Imprisonment for two years, or both	• s 62 of PPIP Act • s 68 of HRIP Act
It is a criminal offence for a person to offer to supply Personal or Health Information that has been disclosed unlawfully	• Fine of up to 100 penalty units ($11,000), or • Imprisonment for two years, or both	• s63 of PPIP Act • s69 of HRIP Act
It is a criminal offence for a person – by threat, intimidation or misrepresentation – to persuade or attempt to persuade an individual: • to refrain from making or pursuing a request to access Health Information, a complaint to the Privacy Commissioner or the NSW Civil and Administrative Tribunal, or an application for an internal review; or • to withdraw such a request, complaint or application.	• Fine of up to 100 penalty units ($11,000)	• s 70(1) of HRIP Act
A person must not – by threat, intimidation or misrepresentation – require another person to give consent under HRIPA, or require a person to do, without consent, an act for which consent is required.	• Fine of up to 100 penalty units ($11,000)	• s 70(2) of HRIP Act
It is a criminal offence for a person to: • wilfully obstruct, hinder or resist the Privacy Commissioner or a member of the staff of the Privacy Commissioner • refuse or wilfully fail to comply with any lawful requirement of the Privacy Commissioner or a member of the staff of the Privacy Commissioner, or • wilfully make any false statement to or mislead, or attempt to mislead, the Privacy Commissioner or a member of the staff of the Privacy Commissioner in the exercise of their functions under the PPIP Act or any other Act	• Fine of up to 10 penalty units ($1,100)	• s 68(1) of PPIP Act

In addition to the above, under section 308H of the Crimes Act 1900 (NSW), it is an offence to access or modify restricted data held in a computer where authorisation has not been provided. The maximum penalty is two years' imprisonment.

Appendix A

Definitions

Affiliate includes contractors, agents, visitors, honorary, clinical or adjunct appointees and consultants of the University.

Collection refers to the way in which the University acquires Personal or Health Information. Collection can be through a written or online form, a verbal conversation, a voice recording, or a photograph.

Controlled Entity/Entities means a person, group of persons or body of which the University or the University Council has control within the meaning of Section 39 (IA) or 45A (IA) of the Government Sector Audit Act 1983 (NSW).

Disclosure refers to sharing information that is held by the University with another agency or individual external to the University.

Health Information, *as defined in Health Records and Information Privacy Act 2002, is:*
"(a) personal information that is information or an opinion about:
the physical or mental health or a disability (at any time) of an individual; or
an individual's express wishes about the future provision of health services to him or her; or
a health service provided or to be provided to an individual; or
(b) other personal information collected to provide, or in providing a health service; or
(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances; or
(d) other personal information that is genetic information about an individual arising from a health service provided to the individual that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual; or
(e) healthcare identifiers."

Personal Information, *as defined in Privacy and Personal Information Protection Act 1998, is:*
"information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics."

It does not include (this list is not exhaustive):

i. *information about an individual who has been dead for more than thirty (30) years;*

ii. *information about an individual that is contained in a publicly available publication;*

iii. *information or an opinion about an individual's suitability for appointment or employment as a public sector official; or*

iv. *information about an individual that is contained in a public interest disclosure, health information within the meaning of Health Records and Information Privacy Act 2002.*

Sensitive Information, as defined in *Privacy and Personal Information Protection Act 1998),* means an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.

Staff means all persons employed by Macquarie University, including continuing, fixed term, and casual Staff members.

Student means any undergraduate, postgraduate, graduate research, or non-award Student currently enrolled or formerly enrolled at the University, whether based on or off-campus.