Privacy Policy

Section 1 - Purpose

(1) Macquarie University (the University) is committed to protecting the privacy of its students, employees and others who interact with it while undertaking its learning and teaching, research, engagement, and associated administrative activities and support services. All staff and functional units of the University have an obligation to be aware of and implement the privacy principles and practices established by legislation and articulated in this and other related policies.

(2) This Policy provides guidance on the University's approach to its information handling practices and that of its Controlled Entities in relation to the information collected from its students, employees and others who interact with it.

Background

(3) As a NSW public sector agency, the University is required to comply with the NSW Privacy and Personal Information Protection Act 1998 (PPIPA) and the NSW Health Records and Information Privacy Act 2002 (HRIPA), in respect of Personal and Health Information it collects and uses. The University aligns its practices and activities with the Information Protection Principles (IPPs), and the Health Privacy Principles (HPPs) contained in those Acts as outlined in the University's Privacy Management Plan.

(4) The University also follows any public interest directions and statutory guidelines issued by the Information and Privacy Commission NSW (or its equivalent) in relation to Personal and Health Information. The University's Privacy Management Plan provides more information on how the University implements its obligations under the PPIPA and HRIPA, and how these Acts apply to the University's operations.

(5) The University's Controlled Entities considered an "organisation" under the Privacy Act 1988 (Cth) (Commonwealth Privacy Act) must also comply with the Commonwealth Privacy Act 1988 and the Australian Privacy Principles (APPs) in addition to the PPIPA and the HRIPA when dealing with Personal and Health Information.

(6) 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. The University's Privacy Management Plan provides more information on the circumstances where GDPR applies to the University's activities and how the University complies with the GDPR obligations.

(7) Whilst the University is not bound to comply with the Commonwealth Privacy Act 1988 (other than as a tax file number recipient), it strives to apply the APPs to its own practices to achieve consistency in protecting the privacy of individuals across University entities.

(8) The University has established the following information Privacy Framework to communicate the applicable privacy laws to staff, students and others who interact with the University:

a. this Policy;
b. Privacy Management Plan;
c. privacy policies for Controlled Entities;
d. privacy collection notices/statements and consents; and

e. related policies, procedures, and guidelines on the management of information.

Scope

(9) This Policy applies to:

a. all employees of the University and its Controlled Entities;
b. all students of the University including former students;
c. all University researchers and graduate research candidates; and
d. any person who handles Personal or Health Information for or on behalf of the University or its Controlled Entities, including contractors, agents, visitors, honorary, clinical or adjunct appointees and consultants of the University.

Section 2 - Policy

(10) The University ensures those covered by the scope of this Policy are made aware of their responsibilities under the PPIPA, HRIPA, and the Commonwealth Privacy Act 1988 and provides appropriate information and training opportunities.

Privacy Management Plan

(11) The University has implemented a Privacy Management Plan setting out how its obligations under PPIPA and HRIPA apply to the University's operations.

Controlled Entities

(12) Each Controlled Entity of the University, considered as an "organisation" under the Commonwealth Privacy Act 1988, is required to have its own separate Privacy Policy.

(13) The Privacy Policy explains the types of Personal and Sensitive (including Health) Information it collects and holds, how it does so, the purposes for that collection, to whom it discloses that Information, how that Information may be accessed or corrected, how a privacy complaint may be lodged and how it will be actioned, whether Information is likely to be sent overseas and to which countries if applicable.

Dealings Between the University and Controlled Entities

(14) The University must ensure that any information provided by the University to a Controlled Entity is protected in accordance with the same standards that the University applies to the information it holds.

(15) Therefore in any dealings between the University and its Controlled Entities regarding Personal and Health Information, the standards applicable to the University (i.e. under PPIPA and HRIPA) must be applied in addition to the requirements under the Commonwealth Privacy Act 1988.

Concurrent Operation of Acts for Controlled Entities

(16) The Commonwealth Privacy Act 1988 contemplates that an entity, such as a Controlled Entity of the University, may have duties under both Commonwealth and State privacy legislation.

(17) To the extent that there are inconsistencies between the Commonwealth Privacy Act 1988 and the NSW privacy acts which apply to a Controlled Entity, the Commonwealth Privacy Act 1988 will prevail.

Privacy Principles

(18) In handling Personal and Health Information, the University and its Controlled Entities align their practices with the IPPs, HPPs and APPs as follows. Where there are additional requirements due to differences between the PPIPA and Commonwealth Privacy Act 1988, specifically the classification of Health Information as Sensitive Information by the Commonwealth Privacy Act 1988 these have also been articulated below.

Collection and Use

(19) The University and its Controlled Entities may collect and use Personal and Health Information only for lawful purposes that are directly related to a function or activity of the University or Controlled Entity, and where the Information is reasonably necessary for that purpose; for a directly related purpose that the individual would expect; or for a purpose for which the individual has given consent, unless an exemption applies.

Disclosure

(20) The University may disclose information held about an individual under various circumstances including the following:

a. if 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; or
b. the individual concerned is reasonably likely to have been aware or is aware that information of that kind is usually disclosed to that party; or
c. the University believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious or imminent threat to an individual's life or health; or
d. consent has been given by the individual; or
e. disclosure is otherwise authorised, permitted, or required by law.

(21) The University cannot disclose an individual's Sensitive Information without consent unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of an individual. For Controlled Entities, this also includes Health Information.

(22) The University publishes graduation information each year, including the full name of the graduating student, the award conferred and the date of conferral. The University regards this as public information. In exceptional circumstances, graduates may contact the Graduations Unit to consider a request to remove their name from the Register.

Transborder Disclosure by University

(23) In addition to the normal disclosure rules, the University will not disclose (or transfer) Personal or Health Information of individuals to any person or body outside NSW or overseas unless an exemption applies.

(24) More specific information about the University's disclosure obligations are available in the Privacy Management Plan.

Cross Border Disclosure by Controlled Entities

(25) Controlled Entities can only use and disclose Personal Information for a purpose for which it was collected ("primary purpose") or for a secondary purpose if an exemption applies.

(26) Generally, the University's Controlled Entities do not disclose Personal Information (including Sensitive Information) outside Australia.

(27) However, some service providers do operate overseas or use third party hosting arrangements that store Information outside Australia. If this occurs, the Controlled Entity is required to take reasonable steps to ensure the overseas recipients treat the Personal Information in accordance with the Australian Privacy Principles and make that overseas recipient accountable if the Information is mishandled.

Collection, Use and Disclosure for Research Purposes

(28) The University may collect, use and disclose Personal or Health Information for research purposes without obtaining an individual's consent provided it complies with:

a. all the criteria set out in section 27B of the PPIPA for Personal Information (or HPP10(1)(f) and HPP11(1)(f) of HRIPA for Health Information);
b. any statutory guidelines issued by the Information and Privacy Commission NSW; and
c. obtains prior approval from the University's Human Research Ethics Committee (Medical Sciences) or Human Research Ethics Committee (Human Sciences and Humanities).

(29) The University's Controlled Entities must also comply with any guidelines issued under sections 95 and 95A of the Commonwealth Privacy Act 1988 in respect of collecting, using and disclosing Health Information for research purposes, or for compilation or analysis of statistics relevant to public health or public safety where individual consent is not obtained, and obtain prior approval of the University's Human Research Ethics Committee (Medical Sciences) or Human Research Ethics Committee (Human Sciences and Humanities).

Retention, Security and Disposal

(30) The University and its Controlled Entities will retain information for as long as necessary for the purpose for which it may lawfully be used, subject to the requirements of any other law.

(31) The University and its Controlled Entities will take reasonable measures to protect information held against loss, misuse, interference and unauthorised access, modification or disclosure.

(32) The University and its Controlled Entities may need to retain records for a significant period of time to comply with their legal obligations. Information that is no longer required will be archived in accordance with the University's retention obligations or securely destroyed in accordance with the University's disposal procedures.

(33) The University may engage a third-party who may hold Personal or Health Information. Where it does so the agreement with the third-party should include provisions for the security, retention and disposal of the information. The third-party contracts should also include obligations to comply with all relevant privacy legislation, where applicable. The completion of a Privacy Impact Assessment should be considered prior to engaging with the third-party.

Access and Correction

(34) An individual may apply to the University or its Controlled Entities to access, correct or amend Personal Information held about them without excessive delay or expense, subject to any exceptions in relevant legislation.

(35) All requests for access should follow the Request for Information process as outlined in the Privacy Management Plan and the Applying to Access Personal Information Guidance Note. Note that access to information about a third party is not accessible under the PPIPA and Commonwealth Privacy Act 1988.

(36) Requests to correct Personal Information can be made informally or through a formal process as outlined in the Privacy Management Plan.

GIPA Access Requests for Information

(37) Any individual may also request access to University records and information held by the University (but not a Controlled Entity) under the Government Information (Public Access) Act 2009 (NSW) (GIPA request).

(38) Under PPIPA and HRIPA access to information is provided only to the person to whom the information relates.

(39) A GIPA request can be made to the University about any information it holds by contacting the Right to Information Officer by email at gipa@mq.edu.au.

Privacy Impact Assessments (PIAs)

(40) Staff should adopt a privacy by design approach when implementing or reviewing a project, process, service or system that involves the handling of Personal Information. Where appropriate, a privacy impact assessment should be undertaken to address privacy risks and issues. The Privacy Impact Assessment Guidance Note provides further information on when a privacy impact assessment should be completed and how to conduct it.

Data Breaches

(41) The University complies with mandatory data breach notification provisions of applicable laws. Identified or suspected data breaches must be reported in a timely manner and handled in accordance with the University's Data Breach Policy.

Complaints

(42) Complaints about privacy breaches by the University are handled in accordance with the University's Privacy Management Plan.

(43) Complaints about privacy breaches by the Controlled Entities are handled in accordance with the relevant Controlled Entity's Privacy Policy.

(44) If an individual has a complaint about how their Personal or Health Information is collected, held, used, secured or disclosed by the University they should contact the University's Privacy Officer in the first instance as follows:

a. Email: privacyofficer@mq.edu.au;
b. Mail: University Privacy Officer, Macquarie University NSW 2109; or
c. Phone: 9850 7218.

Section 3 - Procedures

(45) Nil.

Section 4 - Guidelines

(46) Nil.

Section 5 - Definitions

(47) The following definitions apply for the purpose of this Policy:

a. Controlled Entity/Entities means a person, group of persons or body over which the University has control as

defined in Section 16A of the Macquarie University Act 1989 (as amended) and Section 2.2 of the Government Sector Finance Act 2018.

b. 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."

c. Health Information (for Controlled Entities), as defined in the Commonwealth Privacy Act 1988, is:
"(a) information or an opinion about:
(i) the health, including an illness, disability or injury, (at any time) of an individual; or
(ii) an individual's expressed wishes about the future provision of health services to the individual; or
(iii) a health service provided, or to be provided, to an individual;
that is also personal information;
(b) other personal information collected to provide, or in providing, a health service to an individual;
(c) other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances;
(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual."

d. 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.

e. Personal Information (for Controlled Entities), as defined in the Commonwealth Privacy Act 1988, is:
"information or an opinion about an identified individual, or an individual who is reasonably identifiable:
(a) whether the information or opinion is true or not; and
(b) whether the information or opinion is recorded in a material form or not."

f. Personal 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.

g. Sensitive Information (for Controlled Entities), as defined in the Commonwealth Privacy Act 1988, is:
"(a) information or an opinion about an individual's:
(i) racial or ethnic origin; or

(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual orientation or practices; or
(ix) criminal record;
that is also personal information; or
(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information; or
(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
(e) biometric templates."

Status and Details

Status	Current
Effective Date	30th August 2024
Review Date	29th August 2027
Approval Authority	General Counsel
Approval Date	29th August 2024
Expiry Date	Not Applicable
Responsible Executive	James Lonsdale General Counsel
Responsible Officer	Sophie Buck Director, Governance Services
Enquiries Contact	Rebecca Jarman Compliance and Privacy Manager