Privacy Policy

Section 1 - Purpose of Policy

(1) The University of Wollongong ("the University"), in carrying out its functions and activities, has an obligation to manage an individual's personal information and health information in compliance with NSW privacy laws.

(2) The purpose of this Policy is to set out:

a. the University's commitment to complying with the Privacy and Personal Information Protection Act 1998 and the Health Records and Information Privacy Act 2002 which may include regulations, statutory guidelines, codes of practice and privacy directions made under those Acts;
b. the University's commitment to complying with other privacy laws as they apply to the University's activities and functions;
c. an individual's entitlement to raise concerns regarding the University's handling of their Information; and
d. the responsibilities of the University, its staff and affiliates.

(3) This Policy is implemented by the Privacy Management Plan which operates as a procedure document under the University's policy framework.

Section 2 - Application and Scope

(4) This Policy applies to the collection, storage, access, use and disclosure of Information (see definition of this term) by the University and its staff and affiliates.

(5) All staff and affiliates must comply with this Privacy Policy and the Privacy Management Plan.

(6) A breach of this Policy or the Privacy Management Plan may constitute misconduct pursuant to University codes, policies and guidelines and may be subject to disciplinary action.

(7) This Policy does not apply to the University's controlled entities. The University's controlled entities have their own policies and procedures for the management of Information provided to or collected by them.

Section 3 - The University's Commitment to Privacy

(8) The University is committed to complying with the Privacy and Personal Information Protection Act 1998 and the Health Records and Information Privacy Act 2002, which may include regulations, guidelines, codes of practice and privacy directions made under those Acts. The Privacy and Personal Information Protection Act 1998 and the Health Records and Information Privacy Act 2002 contain principles that regulate the handling of an individual's Information and cover its collection, storage, use, disclosure and rights of access/amendment.

(9) The Privacy Management Plan, prepared in compliance with section 33 of the Privacy and Personal Information Protection Act 1998, sets out:

a. how the University manages its obligations under the Privacy and Personal Information Protection Act 1998, the Health Records and Information Privacy Act 2002 and other applicable privacy laws;
b. how the University disseminates its policies and practices regarding privacy at the University;
c. how an individual can request access to or make amendments to their Information held by the University; and
d. how an individual may make a privacy complaint or lodge a request for formal review of the University's conduct if dissatisfied with the University's handling of their Information, and how such complaints must be managed.

(10) The University's Data Breach Policy sets out strategies to respond to a suspected or known data breach in accordance with obligations under the relevant mandatory notification provisions such as the NSW Mandatory Notification of Data Breach Scheme and is committed to complying with the obligations under relevant privacy laws.

Section 4 - Collection of Information

(11) The University must only collect Information for a lawful purpose that is directly related to one of its functions or activities, and only if the collection is reasonably necessary for that purpose. The University must not collect Information by any unlawful means.

(12) The University must take such steps as are reasonable in the circumstances (having regards to the purposes for which the information is collected) to ensure that the Information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete and does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

(13) The University must, in collecting Information, collect the Information directly from the individual to whom the information relates, unless:

a. the individual has authorised the collection of their Information from someone else; or
b. in the case where a person is under 16 years of age, the Information is provided by the parent or guardian of the person.

(14) The University must when collecting Information from an individual, take such steps as are reasonable in the circumstances to ensure that, before the Information is collected or as soon as practicable after collection, the individual to whom the Information relates is made aware of the following:

a. the fact that the Information is being collected;
b. the purposes for which the Information is being collected;
c. the intended recipients of the Information;
d. whether the supply of the Information by the individual is required by law or is voluntary, and any consequences for the individual if the Information (or any part of it) is not provided;
e. the existence of any right of access to, and correction of, the Information; and
f. the name and address of the agency that is collecting the Information and the agency that is to hold the Information.

(15) The Privacy Management Plan provides further detail concerning collection of Information.

Section 5 - Access, Accuracy and Amendment of

Information

(16) Where the University holds personal information the University must not use the Information without taking such steps as are reasonable in the circumstances to ensure that, having regards to the purpose for which the Information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

(17) The University must respond to enquiries from an individual as to whether it holds that individual's Information including the nature of the Information, the main purpose for the University's use of that Information and any rights of access to it.

(18) The University must allow an individual to:

a. access their own Information;
b. without unreasonable delay or expense;
c. request that appropriate amendments, corrections or updates are made to their Information to ensure that it is accurate and remains relevant, up to date, complete and not misleading (having regard to the purpose for which it was collected and is to be used by the University).

(19) The Privacy Management Plan provides further detail concerning access, accuracy and amendment of Information.

Section 6 - Retention and Security of Information

(20) The University must ensure that Information it collects is:

a. kept for no longer than is necessary for the purpose for which it may lawfully be used and in order to meet its legal obligations;
b. disposed of securely and in accordance with the retention and disposal requirements under the State Records Act 1998 and Records Management Policy; and
c. 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.

(21) The Privacy Management Plan provides further detail concerning retention and security of Information.

Section 7 - Use of Information

(22) In general terms, 'use' of Information refers to the communication or handling of that Information within the University.

(23) The University must only use Information for the primary purpose for which it was collected unless:

a. the use of the Information is directly related to the primary purpose for which it was collected; or
b. the use of the personal information is necessary to deal with a serious and imminent threat to any individual's life or health; or
c. the use of the health information is necessary to deal with a serious and imminent threat to any individual's life, health or safety, or is necessary to lessen or prevent a serious threat to public health or public safety; or
d. the individual provides consent to another use; or
e. the use is permitted by provisions of the Privacy and Personal Information Protection Act 1998 and/or the Health

Records and Information Privacy Act 2002 relating to law enforcement and other related matters; or

f. the use is permitted or required under an Act or any other law; or
g. the use is for the purpose of assisting in a stage of an emergency, it is reasonably necessary for that purpose, and it is unreasonable or impracticable to seek the consent of the individual; or
h. the use is reasonably necessary for the purpose of research or the compilation of statistics in the public interest and:
    i. either the purpose cannot be served by de-identified Information and it is impracticable to seek the consent of the individual for the use, or reasonable steps have been taken to de-identify the Information; and
    ii. if it could reasonably be expected to identify individuals, the Information is not published in a publicly available publication; and
    iii. the use is in accordance with any guidelines issued by the NSW Privacy Commissioner.
i. for health information, where the use is reasonably necessary for research or for the training of employees or persons working with the University and:
    i. either the purpose cannot be served by de-identified Information and it is impracticable to seek the consent of the individual for the use, or reasonable steps are taken to de-identify the Information; and
    ii. if it could reasonably be expected to identify individuals, the Information is not published in a generally available publication; and
    iii. the use is in accordance with any guidelines issued by the NSW Privacy Commissioner.

(24) The Privacy Management Plan provides further detail concerning use of Information and other circumstances where the University may use Information without an individual's consent.

Section 8 - Disclosure of Information

(25) In general terms, 'disclosure' of Information refers to the communication or transfer of Information outside the University.

(26) The University must not disclose Information it holds unless specifically permitted to do so under the Privacy and Personal Information Protection Act 1998 or Health Records and Information Privacy Act 2002. Some of the circumstances may include:

a. the disclosure of the Information is directly related to the primary purpose for which it was collected and there is no reason to believe that the individual concerned would object to the disclosure; or
b. the individual is reasonably likely to have been aware, or has been made aware, that Information of that kind is usually disclosed to a third party; or
c. the disclosure of the personal information is necessary, on reasonable grounds, to prevent or lessen a serious and imminent threat to the life or health of any individual; or
d. the disclosure of the health information is necessary to deal with a serious and imminent threat to any individual's life, health or safety, or is necessary to lessen or prevent a serious threat to public health or public safety; or
e. the individual provides consent to any other disclosure; or
f. disclosure is permitted by provisions of the Privacy and Personal Information Protection Act 1998 and/or the Health Records and Information Privacy Act 2002 relating to law enforcement and related matters such as:
    i. disclosing Information to a law enforcement agency for the purpose of ascertaining the whereabouts of an individual who has been reported to police as a missing person; or
    ii. disclosing Information to an investigative agency as a result of an investigation from a complaint or other

matter that was referred from an investigative agency or that could have been referred or made by the University to the investigative agency; or

g. the disclosure is necessary to assist in a stage of an emergency and it is unreasonable or impracticable to seek the consent of the individual to whom the Information relates; or
h. the disclosure is for the purpose of assisting in a stage of an emergency, it is reasonably necessary for that purpose, and it is unreasonable or impracticable to seek the consent of the individual; or
i. disclosure is permitted or required under an Act or any other law; or
j. the disclosure is reasonably necessary for the purpose of training, research, or the compilation of statistics, in the public interest, and:
    i. either the purpose cannot be served by de-identified Information, and it is impracticable to seek the consent of the individual for the disclosure, or reasonable steps have been taken to de-identify the information; and
    ii. if it could reasonably be expected to identify individuals, the Information is not published in a publicly available publication; and
    iii. the use is in accordance with any guidelines issued by the NSW Privacy Commissioner.

(27) The University must not disclose Information to any person or body who is in a jurisdiction outside NSW or to a Commonwealth agency unless:

a. the University reasonably believes that the recipient of the Information is subject to a law, binding scheme or contract that upholds the principles for the fair handling of the Information that are substantially similar to the principles of NSW privacy laws; or
b. the individual expressly consents to the disclosure; or
c. the disclosure is necessary for the performance of a contract between the individual and the University, or for the implementation of pre-contractual measures taken in response to the individual's request; or
d. the disclosure is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the University and a third party; or
e. all of the following apply:
    i. if it were practicable to obtain such consent, the individual would be likely to give it; or
    ii. it is impracticable to obtain consent of the individual to that disclosure,
    iii. the disclosure is for the benefit of the individual,
f. the disclosure is reasonably believed by the University to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person; or
g. the University has taken reasonable steps to ensure that the Information that it has disclosed will not be held, used or disclosed by the recipient of the Information inconsistently with the information protection principles; or
h. the disclosure is permitted or required by an Act (including an Act of the Commonwealth) or any other law; or

(28) The University must only disclose sensitive Information with the consent of the individual unless disclosure is necessary to deal with a serious and imminent threat to any individual's life or health.

(29) The Privacy Management Plan provides further detail concerning disclosure of Information and other circumstances where the University may disclose Information without an individual's consent or appropriate prior notice.

Section 9 - Anonymity and Identifiers

(30) In relation to health information, the University must:

a. provide individuals with the option of receiving health services or entering into transactions anonymously, wherever it is lawful and practicable; and/or
b. assign a unique identification number to an individual, if the assignment of identifiers is reasonably necessary to enable the University to carry out its functions efficiently.

(31) The Privacy Management Plan provides further detail concerning anonymity and identifiers relating to health information.

Section 10 - Application of Commonwealth Privacy Act and Other Relevant Privacy Laws

(32) The University is a statutory corporation established under the University of Wollongong Act 1989 and as such, is not an agency that falls within the scope of the Privacy Act 1988. However, in some circumstances, Information handled by the University may be expressly governed by the Privacy Act 1988. These circumstances may include:

a. where the University collects tax file numbers from students, staff and affiliates;
b. via the University's contractual interactions with Commonwealth funding agencies;
c. through the University's IT service delivery to its controlled entities; and
d. to meet compliance obligations under relevant Commonwealth legislation such as the Higher Education Support Act 2003 relating to Commonwealth assistance to students.

(33) The Privacy (Australian Government Agencies – Governance) APP Code 2017, requires all Australian Government agencies (as defined by s 5 of the Privacy (Australian Government Agencies – Governance) APP Code 2017) to have a designated Privacy Officer and a designated Privacy Champion.

(34) The University may also have obligations under the (EU) General Data Protection Regulation 2016/679 (GDPR) and other foreign laws in relation to the University's functions and activities. The Privacy Management Plan provides further detail regarding the University's commitment to managing its obligations under the GDPR and other relevant privacy laws as they apply to the University's functions and activities.

Section 11 - Complaints and Enquiries

(35) All privacy enquiries should be directed to the University's Privacy Officer via email at icu-enquiry@uow.edu.au. Additional contact details can be found on the University's Privacy homepage.

(36) If an individual has any concerns about the way the University is managing their Information or believes that the University may have breached their privacy, that individual may:

a. lodge a complaint with a the University's Privacy Officer; or
b. submit a formal request for an internal review of the University's conduct by completing a Privacy Complaint Internal Review Application Form; or
c. contact the Information and Privacy Commission NSW.

(37) For more information about lodging a complaint and/or requesting an internal review of the University's conduct, please see the Privacy Management Plan or visit the University's Privacy homepage.

Section 12 - Roles and Responsibilities

(38) The University's designated Privacy Champion is the Vice-President Operations who is responsible for the following functions:

a. promoting a culture of privacy within the University that values and protects personal information; and
b. providing leadership within the University on broader strategic privacy issues.

(39) The General Counsel as Principal Privacy Officer is responsible for:

a. overseeing the implementation and review of this Policy and the Privacy Management Plan;
a. providing reports to the University's Executive about any privacy issues arising from the University's handling of personal information; and
b. overseeing and deciding the outcome of privacy internal reviews conducted under the Privacy and Personal Information Protection Act 1998.

(40) The University's Privacy Officers in the Information Compliance Unit are responsible for:

a. administering the University's privacy compliance program;
b. implementing and reviewing this Policy and the Privacy Management Plan; and
c. conducting internal reviews of privacy complaints.

(41) Further information regarding the role of the University's Privacy Officers can be found in the University's Privacy Management Plan.

(42) All staff and affiliates are responsible for:

a. complying with the University's privacy obligations and practices as specified in this Policy, the Privacy Management Plan and the University's Code of Conduct when handling Information; and
b. attending and completing privacy training to ensure that the principles of privacy best practice are maintained when handling Information.

(43) Staff and affiliates should be aware that:

a. a breach of this Policy may constitute misconduct pursuant to the University's codes, policies and guidelines and may be subject to disciplinary action.
b. for any research which involves the collection, use or disclosure of Information, ethics review may be required. Further information can be found in the Privacy Management Plan or by contacting a University Privacy Officer.

Section 13 - Definitions

Word/Term	Definition
Affiliate	Includes people holding University of Wollongong Honorary Awards as conferred by the University Council, including the awards of Emeritus Professor, Honorary Doctor and University Fellow; people appointed in accordance with the University's Appointment of Visiting and Honorary Academics Policy; and people engaged by the University as agency staff, contractors, volunteers and work experience students.
Controlled Entity	Controlled Entities are those entities over which the University has control, as defined in section 15A of the University of Wollongong Act 1989 (as amended) and section 1.2(1) of the Government Sector Finance Act 2018.

Word/Term	Definition
Health information	Health information, for the purpose of this Policy, refers to health information defined in the Health Records and Information Privacy Act 2002 (or as amended in the Health Records and Information Privacy Act 2002 from time to time) as 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 1. other personal information collected to provide, or in providing, a health service, or 2. 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 3. other personal information that is genetic information about an individual arising from a health service provided to the individual in a form 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 healthcare identifiers.
Information	Health information and/or personal information as the context permits.
Law Enforcement Agency	As defined in the Privacy and Personal Information Protection Act 1998 and/or the Health Records and Information Privacy Act 2002 as the context applies.
Personal information	Personal information, for the purpose of this policy, refers to personal information defined in the Privacy and Personal Information Protection Act 1998 (or as amended in the Privacy and Personal Information Protection Act 1998 from time to time) as: "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." Under the Privacy and Personal Information Protection Act 1998, personal information does not include: 1. information regarding an individual who has been deceased for more than 30 years; 2. information about an individual that is readily available in a publicly available publication; and 3. information or an opinion about an individual's suitability for appointment or employment as a public sector official.
Sensitive information	A subclass of personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.
Staff	All people employed by the University including conjoint appointments, whether on continuing, permanent, fixed term, casual or cadet or traineeship basis.

Status and Details

Status	Current
Effective Date	8th August 2024
Review Date	8th August 2025
Approval Authority	University Council
Approval Date	8th August 2024
Expiry Date	Not Applicable
Responsible Executive	Stephen Phillips Vice-President Operations
Responsible Officer	Rebecca Lim General Counsel
Enquiries Contact	Information Compliance Unit