Privacy Policy

Version	Approved by	Approval date	Effective date	Next review
1.0	President and Vice-Chancellor	15 October 2019	15 October 2019	October 2022

Policy Statement	
Purpose	This Policy: (a) provides a framework for the University to protect personal information that it holds in compliance with applicable laws; (b) articulates roles and responsibilities for the management of personal information held by the University; and (c) meets the statutory requirement for the preparation and implementation of a University privacy management plan.
Scope	This Policy applies to all staff and affiliates of the University. Controlled entities of the University will manage personal information in accordance with laws applicable to that entity.

Policy Provisions

1. Legislative Framework

1.1 As a body corporate established by a New South Wales Act, the University is primarily bound by New South Wales privacy law, specifically the:

(a) *Privacy and Personal Information Protection Act 1998* (NSW) (the "PPIP Act"); and

(b) *Health Records and Information Privacy Act 2002* (NSW) (the "HRIP Act").

Part 3 of this policy constitutes the University's Privacy Management Plan for the purpose of section 33 of the PPIP Act.

1.2 Other privacy laws that impose obligations on the University include the:

(a) *Privacy Act 1988* (Cth), in regard to the University's handling of tax file numbers (TFNs) (Privacy Act)

(b) *European Union General Data Protection Regulation* (2016/679) (the "GDPR"), in regard to the University's handling of personal information of EU residents.

2. Policy Statement

2.1 The University is committed to protecting personal information in compliance with all applicable laws, and incorporates applicable legal requirements into the University's processes, procedures and information systems.

2.2 The University:

(a) manages all personal information that it holds in accordance with the Information Protection Principles (IPPs) prescribed by the PPIP Act

(b) manages all health information that it holds in accordance with the Health Privacy Principles (HPPs) prescribed by the HRIP Act

(c) manages TFNs in accordance with the Privacy Act

(d) where required, processes personal information collected from EU residents in accordance with the requirements of the GDPR.

2.3 Personal information and health information that is collected and held by the University is:

(a) collected for specified and lawful purposes only and not used for any unauthorised purpose

(b) limited to what is necessary for the purposes for which the personal and health information have been collected and the University will take reasonable steps to ensure that the information which it holds is up to date, accurate and relevant to the purpose for which it has been collected

(c) available to be accessed and, on request, amended by the person to whom the personal and health information relates

(d) used and disclosed lawfully

(e) kept in a form which permits identification of individuals for only as long as is necessary for the purposes for which it was collected (except where such information is required to be kept for a longer period by law) and disposed of securely once it is no longer required

(f) used, disclosed and stored in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful use and disclosure and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Privacy Management Plan

3.1 The Policy is supported by:

(a) approved procedures, guidelines and privacy collection statements that support implementation of this policy

(b) privacy awareness training available for all University staff.

3.2 This Policy, and supporting documents, are publicly available on the University's website.

3.3 The University implements procedures under this policy to enable it to respond lawfully to applications for internal review of privacy complaints made under section 53 of the PPIP Act.

3.4 The University verifies compliance with relevant privacy obligations, reports incidents of non-compliance and addresses such incidents in a timely and effective manner through the certification and reporting provisions prescribed by the University's *Legislative Compliance Policy* and *Legislative Compliance Procedure*.

3.5 Data breaches involving personal information are managed in accordance with the University's *Data Breach Policy* and its supporting documents. The University complies with mandatory data breach notification provisions of applicable laws.

3.6 The University's website provides:

(a) information about how the University manages the collection, storage and use of personal information and health information

(b) an explanation of individual rights in regard to personal and health information collected by the University and how individuals may exercise such rights

(c) links or forms to enable individuals to access and/or request amendment to their personal or health information held by the University, or to apply for internal review of University conduct in relation to their personal or health information

(d) contact details for the University's Privacy Officer and University Compliance Owners appointed under this policy (see section 4).

4. Roles and Responsibilities

4.1 Members of the University's **Management Board** are responsible for:

(a) overseeing the management of personal and health information within their respective portfolios

(b) assigning performance of the duties prescribed by section 4.2 of this Policy to a **University Compliance Owner/s**[1] for personal and health information held within their portfolio, on the basis that the members of the Management Board remain responsible for the performance of these duties

(c) endorsing the findings and recommendations arising from internal reviews conducted by the University Privacy Officer or other designated University officer (where such reviews concern personal or health information held within their portfolio) and notifying applicants of the outcome of such reviews.

4.2 **University Compliance Owners** (UCOs) assigned under 4.1 are responsible for:

(a) ensuring that University-wide procedures implemented to support this policy are applied in the management of personal and health information within their respective portfolios

(b) implementing effective local procedures to ensure that personal and health information held within their portfolio is managed in accordance with this policy

(c) ensuring that any person who has access to the personal information held within their portfolio understand their responsibilities in regard to such information

(d) ensuring that privacy statements that comply with all applicable laws are provided to individuals when their personal information is collected

4.3 The **University Privacy Officer** is responsible for:

(a) implementation of this Policy

(b) developing and implementing University-wide procedures to support this Policy

(c) supporting the UCOs to develop local protocols and privacy statements for use in their area of responsibility

(d) providing advice to UCOs and other internal stakeholders on the obligations imposed by all applicable privacy laws

(e) developing guidelines, training and other supporting material to support awareness of obligations imposed by applicable privacy laws

(f) conducting internal reviews of privacy complaints received in accordance with section 53 of the PPIP Act.

4.4 **Managers and supervisors** are responsible for ensuring that all staff within their unit handle personal information in accordance with this policy and applicable supporting procedures.

4.5 **Individual staff** are responsible for ensuring that they handle personal information in accordance with this policy and applicable supporting procedures.

[1] Refer to the Legislative Compliance Policy and Legislative Compliance Procedure for more information on the role of University Compliance Owners.

Accountabilities	
Responsible Officer	Deputy Vice-Chancellor Enterprise
Contact Officer	University Privacy Officer, Compliance Unit, Legal Office
Supporting Information	
Legislative Compliance	This Policy supports the University's compliance with the following legislation: *Privacy and Personal Information Protection Act 1998* (NSW) (the "PPIP Act") *Health Records and Information Privacy Act 2002* (NSW) *Privacy Act 1988* (Cth) *EU General Data Protection Regulation* 2016/679
Supporting Documents	
Related Documents	Legislative Compliance Policy Legislative Compliance Procedure Deta Governance Policy Research Data Governance and Materials Handling Policy Date Breach Policy Data Classification Standard Data Handling Guideline zID Usage Guideline Recordkeeping Standard
Superseded Documents	UNSW Privacy Management Plan 2009
File Number	2019/38549
Definitions and Acronyms	
Affiliate	Conjoint and visiting appointees; consultants and contractors; agency staff; emeriti; members of University committees; and any other person appointed or engaged by the University to perform duties or functions for the University.
Staff	All employees of the University, including casual employees.
Student	A person who has accepted an offer to a program of UNSW (award or non-award), has enrolled in at least one course in that program and retains an active status in that program.

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	President and Vice-Chancellor	15 October 2019	15 October 2019	New policy