Privacy Policy

Section 1 - Purpose and Scope

(1) The purpose of this Policy is to set out the University's framework for protecting personal and health information.

(2) This Policy applies to all personal and health information held by the University.

Section 2 - Definitions

(3) Data Breach or Privacy Data Breach means unauthorised access or disclosure of personal information, or loss of personal information.

(4) Health information has the meaning set out in section 6 of the HRIPA; that is, a type of personal information that relates specifically to an individual's health. Health information is information or an opinion about:

a. a person's physical or mental health or disability;
b. a person's express wishes about the future provision of their health services; or
c. a health service provided, or to be provided to a person.

(5) Health Privacy Principles means the principles set out in Schedule 1 of the HRIPA.

(6) HRIPA means the Health Records and Information Privacy Act 2002.

(7) Information Protection Principles means the principles set out in Part 2 Division 1 of the PPIPA.

(8) Personal information has the meaning set out in section 4 of the PPIPA; that is, information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion, irrespective of whether the information is recorded in a material form or not, and including information or an opinion forming part of a database.

(9) Plan means the University's Privacy Management Plan.

(10) PPIPA means the Privacy and Personal Information Protection Act 1998.

Section 3 - Policy Statement

(11) The University will collect, store, provide access to, use and disclose personal and health information in accordance with the PPIPA, the HRIPA and, where applicable, the Privacy Act 1988 (Cth) and the European Union General Data Protection Regulation 2016 (GDPR)

(12) This Policy is supported by:

a. the Privacy Management Plan
b. the Privacy Data Breach Response Process; and

c. the guidelines and information on the University's Privacy and Personal Information webpage.

Privacy Management Plan

(13) The University's Privacy Management Plan sets out how the University complies with the Information Protection Principles and Health Privacy Principles.

(14) The Plan also contains information on how to make a complaint about an alleged breach of privacy, and how to seek internal review of that decision.

(15) The University's Privacy Contact Officer, together with the Legal Office, will keep the Plan current.

(16) The Privacy Contact Officer, or the relevant University Work Unit responsible for the release of personal or health information as set out in the Plan, will respond promptly to applications for access to personal information.

Training

(17) The University will provide regular and ongoing training to University staff about the University's privacy obligations. This training will include:

a. maintaining a Privacy and Personal Information webpage with up to date information about privacy issues; and
b. providing online or face-to-face training to staff on their privacy obligations on both a regular and as needed basis.

Staff responsibilities

(18) All staff must comply with, and implement, the Information Protection Principles, the Health Privacy Principles, this Policy and the Plan, and ensure staff under their supervision, or students under their direction, are made aware of their obligations under these principles, the Policy and the Plan.

(19) Staff must undertake a risk analysis for any new activities or projects that deal with the collection, use or disclosure of personal or health information to assess whether they have the potential to impact on an individual's privacy and, if so, how they will be managed in accordance with the Plan.

(20) Staff, students and affiliates are to report any breach of the Plan to the Privacy Contact Officer, including any instances of accidental collection, misuse, disclosure or destruction of personal or health information.

Data Breaches

(21) All actual or suspected Privacy Data Breaches must be dealt with in accordance with the University's Privacy Data Breach Response Process.

Section 4 - Procedures

(22) Nil.

Section 5 - Guidelines

(23) Nil.

Status and Details

Status	Current
Effective Date	16th December 2019
Review Date	16th December 2025
Approval Authority	Head, Governance Services
Approval Date	16th December 2019
Expiry Date	Not Applicable
Responsible Executive	Allan Morris Vice President (Operations) +61 2 66269220
Head of Work Unit	Mark Dixon Director, Governance Services
Enquiries Contact	Governance Services