Information Management Policy

Section 1 - Purpose and Scope

Purpose

(1) This Policy provides a framework for a whole of University approach to Information Management to:

a. support the University to achieve its strategic objectives;
b. ensure valuable information and data assets are managed appropriately; and
c. ensure the University's compliance with applicable laws, regulations and standards.

Scope

(2) This Policy applies to:

a. all staff, students, contractors and consultants accessing the University's Information; and
b. all University Information.

Section 2 - Definitions

(3) For the purposes of this Policy, the following definitions apply.

a. Information means all information held by the University in any form or format (paper, digital or audio-visual) whether registered files, working papers, electronic documents, emails, online transactions, data held in databases or on tapes or disks, maps, plans, photographs, sound and video recordings or microforms, backup and archived data.
b. Information Area means a subset of University Information that relates to specific function, activity, business process or IT system of the University.
c. Information Asset means a collection of Information defined and managed as a single unit so it can be understood, shared, protected and utilised effectively.
d. Information Asset Register is a register of the Information Assets across the University.
e. Information Custodian means the staff member with data content expertise who oversees an Information Area as assigned by the Vice President (Operations) in accordance with this Policy.
f. Information Handling Requirements mean the business processes to be followed regarding the collection, storage, use, sharing, archiving and disposing of Information as set out in the Information Classification and Handling Guidelines.
g. Information Quality means the validity, relevancy and currency of Information.
h. Information Steward means the staff member appointed to manage Information Quality and Information Handling Requirements for an Information Area.
i. Personal Information means 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 be reasonably ascertained from the information or opinion as defined in the Privacy and Personal Information

Protection Act 1998(NSW).

Section 3 - Policy Statement

(4) Information is an asset that has value to the University and must be managed accordingly.

(5) Accurate and current Information is made available to appropriate users to enable them to conduct University business and support analysis, decision-making and risk identification.

(6) University Information Assets will be classified and managed in accordance with this Policy and the Information Classification and Handling Guidelines.

(7) The University will establish and maintain an Information Asset Register in accordance with this Policy to:

a. ensure the accuracy and integrity of its Information;
b. provide a reference point for users of Information to identify available Information resources; and
c. provide Information Custodians with an overview of the Information under their responsibility.

(8) Information must be kept up-to-date throughout every stage of a business workflow.

(9) Access to Information Assets will be provided to staff who require that Information in order to conduct authorised University business and in accordance with the Information Handling Requirements.

(10) Information should only be collected for legitimate uses directly related to a function or activity of the University. Extraction, manipulation and reporting of Information must only be done to perform University business, including teaching or research.

(11) Information must be retained and disposed of in accordance with:

a. the State Records Act 1998 (NSW) and the University's Records Management Policy and Procedures;
b. any other legislation setting out retention and disposal requirements for specific types of Information.

(12) In applying this Policy, the University must comply with its legislative obligations including the requirements of the Privacy and Personal Information Act 1998 (NSW), the Privacy Act 1998 (Cth) and the Health Records and Information Privacy Act 2002 (NSW).

(13) All University staff, students, contractors and consultants are responsible for complying with this Policy, the Information Classification and Handling Guidelines and any related University policies and procedures.

(14) The Vice President (Operations) is responsible for resolving disputes concerning the classification or handling of Information. Where the dispute involves the collection, use or disclosure of Personal Information, the Privacy Contact Officer must be consulted to ensure compliance with relevant privacy legislation.

Section 4 - Information Classification and Handling

(15) The University has three information classifications:

a. Highly Sensitive

(16) The Vice President (Operations) will approve Information Classification and Handling Guidelines.

Section 5 - Information Stewards and Custodians

Information Custodians

(17) The Vice President (Operations) will assign an Information Custodian for each Information Area. Information Custodians are expected to have high-level knowledge of the content of Information within their Information Area. Information Custodian will normally be a Head of Work Unit or other senior staff member.

(18) Information Custodians are responsible for managing Information in their Information Area.

(19) For each Information Area, Information Custodians will:

a. assign Information Classifications in accordance with Section 6 of this Policy;
b. determine who may access Information Assets classified as Highly Sensitive based on an assessment of the user's need to access the Information Asset to enable them to conduct University business and support analysis, decision-making and risk identification;
c. implement and oversee the business processes to manage Information Assets in the Information Area;
d. audit access processes regularly, referring to the Information Classification and Handling Guidelines for guidance; and
e. report Information Management issues and concerns to the Vice President (Operations).

Information Stewards

(20) The Information Custodian will appoint an Information Steward to oversee the day to day management of Information Assets in an Information Area.

(21) Information Stewards will:

a. support compliance with Information Classification and Handling Guidelines; and
b. maintain Information Quality.

Section 6 - Information Classification and Handling Requirements

(22)

(23) Information Custodians are responsible for classifying Information Assets in their Information Area. The Information must be classified consistently and in accordance with the Information Classification and Handling Guidelines.

(24) For Information Assets classified as Highly Sensitive or Sensitive, the classification must be reviewed by the Information Custodian every three years.

Section 7 - Associated Documents

(25) This Policy should be read in conjunction with:

a. Records Management Policy and Record Management Procedures
b. Privacy Policy, Privacy Management Plan and Privacy Data Breach Response Process

c. Information Technology Conditions of Use Policy
d. Research Data Management Policy
e. Open Access Policy
f. Institutional Repository Policy

Status and Details

Status	Not Yet Approved
Effective Date	To Be Advised
Review Date	To Be Advised
Approval Authority	Director, Governance Services
Approval Date	To Be Advised
Expiry Date	Not Applicable
Head of Work Unit	Belinda Atkinson Director, Governance Services +61 2 66203186
Enquiries Contact	Governance Services