THE UNIVERSITY OF NOTRE DAME AUSTRALIA

Policy:

Information and Information Technology

Effective: 8 November 2023

Audience: Employees, students

Policy category: management
Policy sub-category: information management and privacy

Key words:	Cybersecurity, data, information, information security, social media
Policy Owner:	Chief Information Officer
Responsible Officer:	Director, Cybersecurity and Business Partners
Review Date:	August 2025

Contents

1 OBJECTS OF THE UNIVERSITY

1.1 The Objects of the University of Notre Dame Australia (the University) are defined in Section 5 of its Act of Parliament.

1.2 The Objects of the University are:

1.2.1 the provision of university education, within a context of Catholic faith and values; and

1.2.2 the provision of an excellent standard of:

1.2.2.1 teaching, scholarship and research;

1.2.2.2 training for the professions; and

1.2.2.3 pastoral care for its students.

2 PURPOSE

2.1 This policy defines the University's objectives and standards for:

2.1.1 managing information and ensuring its quality

2.1.2 ensuring information security

2.1.3 managing information technology, and

2.1.4 ensuring appropriate use of university information technology.

2.2 The Interpretation and definitions section below:

2.2.1 states requirements for interpreting this policy and

2.2.2 explains its hierarchical relationship with other policy documents in the University's *Policy Framework*.

3 SCOPE

3.1 This policy applies to:

3.1.1 staff of the University

3.1.2 students enrolled in programs and courses offered by the University

3.1.3 anyone else who uses the University's information technology, including adjunct staff, visiting staff, members of the Board of Directors, research associates, emeriti staff, alumni, and consultants and contractors engaged by the University, and

3.1.4 under the circumstances defined in the *Procedure: Information Technology*, staff or students using social media.

3.2 The *Policy: Research Data Management* and *Procedure: Research Data Management* state requirements for managing information received or created in academic research.

3.3 The *Policy: Intellectual Property* applies to intellectual property held on university information systems.

3.4 The *Policy: Privacy* applies to personal information held on university information systems.

3.5 The *Employee Code of Conduct and Ethical Behaviour* and *Code of Conduct (Students)* define expectations of behaviour, including behaviour when using information systems or social media.

4 PRINCIPLES

4.1 Information is one of the University's most important assets.

4.2 Staff who create or change data on university information systems will follow the relevant process instructions to ensure that the data is fit for purpose, enabling the University to:

4.2.1 monitor its performance via business information reporting, and
4.2.2 meet its external reporting obligations for statutory compliance and funding.

4.3 Anyone who uses an information system of the University will keep the information system and its data safe from damage and secure from unauthorised access.

4.4 Some of the information held by the University is private and/or confidential, because
4.4.1 if made public it might
4.4.1.1 be misunderstood, causing a risk of harm to the University's reputation
4.4.1.2 inadvertently release the University's intellectual property or
4.4.1.3 remove a competitive advantage enjoyed by the University, or
4.4.2 it is personal information of a staff member or student which the University has an obligation to keep in confidence.

4.5 Information gathered or created in university activities will be classified to define how it can be used and what arrangements are needed to ensure its security.
4.5.1 There will be four information classification levels:
4.5.1.1 public
4.5.1.2 internal
4.5.1.3 sensitive
4.5.1.4 highly sensitive.
4.5.2 Where there is an actual or suspected breach of the security or confidentiality of university information, the University will respond quickly to assess and manage the breach to minimise harm from it.
4.5.3 The *Procedure: Information Management*
4.5.3.1 defines these classification levels in more detail
4.5.3.2 states requirements for managing information with the different levels of classification, and
4.5.3.3 states how a breach of information confidentiality or information security will be assessed and managed.

4.6 Staff and students are expected, both in their use of university information systems and in their personal use of social media, to avoid
4.6.1 harming the reputation or interests of the University or causing the University to fail to meet its legal responsibilities, or
4.6.2 posting or sharing material that breaches (as relevant) the *Employee Code of Conduct and Ethical Behaviour* or *Code of Conduct (students)*.
4.6.3 The University will monitor use of its information technology and information systems on an ongoing basis, to ensure they are used appropriately.

4.7 This policy is intended to ensure that the University complies with the following legislation, standards and government regulations, policies and guidelines:
4.7.1 Legislation:
- *Health Records and Information Privacy Act 2002* (NSW)
- *Privacy Act 1988* (Commonwealth) and the *Australian Privacy Principles* it contains
- *Privacy Amendment Act 2012* (Commonwealth)
- *Privacy Amendments (Privacy Alerts) Bill 2013* (Commonwealth)
- *Privacy and Personal Information Protection Act* 1998 (NSW)
- *Security of Critical Infrastructure Act* 2018 (Commonwealth)
- *Workplace Surveillance Act* 2005 (NSW)

4.7.2 Standards:
- AS/*NZS*/IEC 270001:2006 *Information Technology – Security Techniques –*

Information Security Management Systems – Requirements

- *ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements*
- *ISO/IEC 27002:2013: Information technology – Security techniques – Code of Practice for Information Security Controls*
- *ISAE No.* 3402*, Assurance Reports on Controls at a Service Organization*
- *NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations*

4.7.3 Government regulations, policies and guidelines

- *Digital Information Security Policy* (NSW)
- *General Data Protection Regulation* (European Union)
- *Government Information Classification and Labelling Guidelines 2013* (NSW).

5 ROLES AND RESPONSIBILITIES

5.1 Everyone who uses a university information system or a device provided by the University will:

5.1.1 maintain the security of the system or device and the information it contains

5.1.2 abide by the terms and conditions for its use, and

5.1.3 in using the system or device, follow instructions to ensure information security and the quality of data set by the Chief Information Officer and/or the business owner of the information system.

5.2 Data Governance Group

5.2.1 The Data Governance Group will:

5.2.1.1 oversee the University's approach to data management, and

5.2.1.2 recommend changes to the *Procedure: Information Management* to the Vice-Chancellor for approval.

5.3 Chief Information Officer:

5.3.1 The Chief Information Officer will:

5.3.1.1 lead and coordinate university activities to ensure the security of information systems, infrastructure and devices

5.3.1.2 maintain detailed instructions for staff to ensure information security, and

5.3.1.3 maintain the University's information security plan for approval by the Vice-Chancellor, and

5.3.1.4 decide change controls for changes to enterprise information systems to minimise disruption to service.

5.4 Operations Group

5.4.1 The Operations Group will oversee expenditure on information technology (see the group's terms of reference for more detail on its role in this).

6 RELATED DOCUMENTS

6.1 The *Procedure: Information Management* states requirements for:

6.1.1 classifying information created or received by the University

6.1.2 managing university information to which access is restricted

6.1.3 ensuring the quality of data on university systems, and

6.1.4 assessing and managing breaches of the confidentiality and/or security of information held by the University.

6.2 The *Procedure: Information Technology* states requirements for managing the University's information technology and ensuring its proper use and security.

6.3 The *Procedure: Social Media* states requirements for use of social media by staff and students of the University.

6.4 The *Employee Code of Conduct and Ethical Behaviour* and *Code of Conduct (Students)* define the behaviours expected of staff and students, which apply in contexts including staff and student use of information systems and private use of social media.

7 INTERPRETATION AND DEFINITIONS

7.1 Interpretation

7.1.1 The following rules of interpretation apply to this policy.

7.1.2 The University's *Policy Framework* sets out the hierarchy of the University's policy documents.

7.1.3 Should any provision in this policy be inconsistent with a provision of a document higher in the University's hierarchy of policy documents as stated in the *Policy Framework*, the higher document prevails and overrules this policy to the extent of the inconsistency.

7.1.4 This policy must be read alongside other closely-related policy documents:

7.1.4.1 the procedures that support this policy, listed in the Related documents section

7.1.4.2 the *Employee Code of Conduct and Ethical Behaviour* and *Code of Conduct (Students)*, which include a requirement to comply with policy documents of the University, and

7.1.4.3 any other documents listed in the Related documents section.

7.1.5 The procedures that support this policy state detailed requirements in relation to the principles stated in this policy.

7.1.5.1 Where a principle stated in this policy implies a service or entitlement to a person, to enjoy the service or entitlement, the person must meet any requirements and/or conditions that a supporting procedure states in relation to the service or entitlement.

7.1.6 Where this policy uses:

7.1.6.1 the verbs 'will' or 'must', it states a requirement

7.1.6.2 the phrases 'cannot', 'must not' or 'only [position title] can', it states a prohibition

7.1.6.3 the words 'include', 'includes; or 'including' followed by a list, the words 'without limitation' are taken to follow immediately

7.1.6.4 the phrase 'for example' or 'such as' followed by a single instance or list, the instance or list is not exhaustive

7.1.6.5 the phrases 'described in', 'set out in', 'specified in' or 'stated in', it will be read as if the words 'expressly or impliedly' appeared immediately before them;

7.1.6.6 the singular, it also means the plural, and vice versa

7.1.6.7 any gender, it includes the other genders, and

7.1.6.8 a reference to a statute, ordinance, code or other law, it includes regulations, by-laws, rules and other statutory instruments under it for the time being in force and consolidations, amendments, re-enactments or replacements of any of them.

7.2 Definitions

7.2.1 For the purpose of this policy, the following definitions apply:

7.2.1.1 ***Data*** means information stored in a digital format such as numbers, texts and scanned documents or images.

7.2.1.2 ***Enterprise information system*** means an information system that the University provides for use enterprise-wide: for example, the finance system, human resources system, learning management system, library system and student management system.

7.2.1.3 ***Information*** means:

- data, and
- hard copy information and other types of physical record held by the University.

7.2.1.4 ***Personal information*** means information or opinion, whether true or not and whether recorded in a material form or not, about an individual, including information that the University holds in relation to students, staff, contractors and information regarding individuals who attend university functions.

7.2.1.5 ***Social media*** mean social networking websites and applications, video and photo sharing websites and applications, blogs, micro-blogging sites, forums and discussion boards, wikis, podcasts, email and instant messages, virtual communities and any other websites or apps that allow users to share comments and/or images over the internet.

7.2.1.6 ***University information system*** means any information system used to create, manage or store information for purposes of the University; enterprise information systems are a subset of university information systems.

Version	Date of approval	Approved by	Amendment
1	2 August 2022	Vice-Chancellor	Effective date – new policy.
2	15 November 2022	Chief Information Officer	Minor amendment (cl. 4.5.1.4).
3	8 November 2023	University Secretary	Consequential edit to add reference to *Employee Code of Conduct and Ethical Behaviour* (replaced Staff Code of Conduct)