THE UNIVERSITY OF NOTRE DAME AUSTRALIA

Procedure:

Information Technology

Effective: 2 August 2022

Audience: employees, students

Policy category: management
Policy sub-category: information technology

Key words:	Information, information security, information technology, IT
Procedure Owner:	Chief Information Officer
Responsible Officer:	Director, Cybersecurity and Business Partner
Review Date:	August 2025

Contents

1 PURPOSE 3
2 RELATED POLICIES AND REGULATIONS 3
3 USER ACCESS 3
4 MONITORING INFORMATION TECHNOLOGY USE 4
5 MOBILE DEVICES 5
6 USERS' OWN DEVICES 7
7 PHYSICAL SECURITY OF INFORMATION TECHNOLOGY 7
8 SOFTWARE DEVELOPMENT AND INSTALLATION 7
9 INFORMATION TECHNOLOGY REGISTER 7
10 BACKUP AND DISASTER RECOVERY 8
11 RESPONSIBILITIES 8
12 RELATED DOCUMENTS 9
13 INTERPRETATION AND DEFINITIONS: 9

1 PURPOSE

1.1 This procedure supports the *Policy: Information and Information Technology* by stating requirements for:

1.1.1 managing information technology of the University of Notre Dame Australia (the University), and

1.1.2 ensuring the proper use and security of the University's information technology.

1.2 The Interpretation and definitions section at the end of this procedure:

1.2.1 states requirements for interpreting this procedure and

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

1.3 Scope

1.3.1 This procedure has the same scope as the *Policy: Information and Information Technology*.

2 RELATED POLICIES AND REGULATIONS

2.1 This procedure should be read alongside the *Policy: Information and Information Technology*, which it supports.

2.2 The *Procedure: Information Management* states requirements for managing information created, received or held by the University, including how:

2.2.1 it will be classified for confidentiality and security, and

2.2.2 any breach of its confidentiality and/or security will be assessed and managed.

2.3 The *Procedure: Social Media* states requirements for:

2.3.1 establishing and managing social media facilities of the University, and

2.3.2 personal use of social media by staff or students.

3 USER ACCESS

3.1 Users of university information systems will be provided with the minimum privileges and access rights they need to perform their role.

3.2 The Office of Information Technology will provide each user of university information and systems with, as relevant, a staff or student account to enable them to have the relevant level of access to the systems relevant to their role.

3.2.1 The user will establish a password for access to their account that complies with password protocols set by the Office of Information Technology.

3.2.2 The user will keep their account username and password secure and not share them with any other person.

3.3 Where someone such as a consultant, contractor or academic visitor needs temporary access to university information and communication systems to carry out their role, the Office of Information Technology will provide them with a temporary account only for the period during which they need the access.

3.4 Where a person or organisation external to the University maintains or supports the University's information technology or software, the Office of Information Technology will provide them with access only to the relevant system(s) and to the extent needed for this work.

3.5 Conditions of access

3.5.1 The Chief Information Officer will maintain terms and conditions of access to a university information technology user access account to ensure that users of university information and communication systems:

3.5.1.1 maintain their security

3.5.1.2 maintain the security and confidentiality of the information the system contains

3.5.1.3 use the system only for the uses for which it is intended, and

3.5.1.4 are aware that their use of the system must comply with the relevant code of conduct.

3.5.2 A business owner of a university information system may maintain supplementary terms and conditions of access to that system.

3.6 Appropriate use of access

3.6.1 A staff user may only access information they need to carry out the functions of their work role.

3.7 Disabling user accounts

3.7.1 When someone ceases to be a staff member, a student or alumnus of the University, or when someone with temporary access to university information and communication systems ceases to need the access, the Office of Information Technology will immediately disable their user account, either:

3.7.1.1 as part of an automated process that will occur when a staff member ceases to be employed or after a student ceases to be enrolled (an offboarding process), or

3.7.1.2 where the change will not be picked up by an automated offboarding process, on notification by the manager responsible for the employment, enrolment or other type of relationship with the University. (Such a manager is responsible for notifying the IT Service Desk promptly of such changes.)

3.7.1.3 In the case of a student becoming a graduate with no current student enrolment, their student user account will be replaced with an alumnus user account.

3.7.1.4 The OIT will collaborate with the Registry and People and Culture to maintain business rules for offboarding (as relevant) students or staff.

3.7.2 Where a user account needs to be disabled immediately for an unexpected reason such as a suspected serious breach of a code of conduct, this must have been authorised by one of the Vice-Chancellor, Provost or Pro Vice-Chancellor, People and Culture.

3.7.2.1 Where the Vice-Chancellor, Provost or Pro Vice-Chancellor, People and Culture are not available to authorise disabling a user's account for such a reason, the Chief Information Officer may authorise disabling it.

4 MONITORING INFORMATION TECHNOLOGY USE

4.1 The University will monitor use of its information systems to ensure users are complying with the terms and conditions of access to the relevant systems.

4.1.1 University information systems generate logs of transactions and usage, which system administrators may use to view the content of electronic communications and files sent and stored.

4.1.2 Even where a user has deleted a file, the University may retain and review archived and/or backup copies of the file.

4.1.3 The Office of Information Technology will monitor internet usage via university information technology infrastructure, including sites and pages visited, files downloaded, video and audio files accessed and data entered, and may access records of these

4.2 The Vice-Chancellor or Chief Information Officer may authorise a staff member to gain access to a staff member's or student's university information and communication systems user account in exceptional circumstances such as:

4.2.1 where the staff member is unexpectedly away, and access to their user account is needed to provide continuity of service, or

4.2.2 to investigate an allegation of misconduct by the staff member or student involving misuse of university information and communication systems.

4.3 For the purposes of the *Workplace Surveillance Act 2005* (Commonwealth), this section constitutes written notice of the University's computer surveillance of its employees.

5 MOBILE DEVICES

5.1 The Procurement team in the Office of Finance (Procurement), in collaboration with the Office of Information Technology (OIT), provides mobile phones and/or tablet computers (mobile devices) to:

5.1.1 university staff who need these to perform their duties

5.1.2 members of the University's Board of Directors, and

5.1.3 independent contractors who need a mobile device provided by the University to carry out the work for which the University has engaged them.

5.2 A new mobile phone will normally be provided to each executive staff member and manager on their appointment to their position.

5.2.1 Where a staff member below manager level needs a mobile device to perform their work duties (for example, where these require them to be contactable while away from their work area and/or outside working hours), an executive staff member in the staff member's line of management reporting may request that they be issued with a device.

5.2.2 In such a case, the staff member will be issued with a device from the pool of available new and used devices.

5.3 Where a staff member who has been issued with a mobile device changes to a different position below the level of manager, their eligibility to have the device will be re-assessed.

5.4 To request a mobile device, a staff member must complete the university form for this purpose, and submit it by the process stated on the form.

5.5 By accepting the issue of a university-provided mobile phone, a staff member is accepting that the mobile phone number may be communicated internally and externally to meet the needs of the University and the purposes for which the phone was provided: for example, the number may be published in the staff directory, on the University's public website and/or in an external publication.

5.6 New mobile devices will be purchased from preferred suppliers of the University, and mobile phones will be connected to the corporate telecommunications carrier and mobile device management platform.

5.6.1 However, an executive staff member may request a different supplier or platform for a staff member's mobile device.

5.6.2 The Chief Financial Officer may approve an exception in such cases.

5.7 The *Procedure: Information Management* authorises the Chief Information Officer (CIO) to

maintain detailed instructions to staff to whom the University issues a mobile device, to ensure:

5.7.1 its security, and

5.7.2 the security and backing up of university information held on or accessed via the device.

5.7.3 The CIO's instructions may also state other requirements for use of a mobile device, as a condition of its provision.

5.8 The University permits reasonable personal use of university-provided mobile devices. Reasonable personal use means use that does not:

5.8.1 incur costs the staff member would be unwilling to pay themselves if the relevant executive staff member considers the costs excessive, or

5.8.2 breach the conditions of use of the device provided to the staff member when it was supplied to them.

5.8.3 The OIT may monitor use of a mobile device it has provided to a staff member, by downloading detailed call and data logs from the relevant telecommunications carrier.

5.8.4 The University will pay the fringe benefit tax, if any, incurred by personal use of a mobile device it has provided to a staff member.

5.8.5 When a staff member is on parental leave or long service leave, the University will continue to pay for their reasonable personal use of a mobile device provided to them by the University.

5.9 Staff who are provided with a mobile phone by the University are expected to avoid incurring unreasonable expenses by their use of the phone.

5.9.1 The CIO's instructions for staff to whom a mobile device is issued provide details of what are considered reasonable and unreasonable expenses.

5.10 Procurement provides global roaming for phonecalls and sending of text messages, for the purposes of international travel on university business.

5.10.1 A request for global roaming beyond the end of a staff member's business travel must have been approved by an executive staff member in the staff member's management reporting line.

5.11 If a staff member loses a mobile device provided by the University, or such a device is damaged or stolen, the staff member will immediately report the loss, damage or theft to both the IT service desk and their line manager.

5.12 Where the phone number of a mobile phone is provided along with the phone, as the contact number for a staff position or staff function (for example, as a contact number for a service to students or staff), the phone number cannot be transferred to a staff member's personal mobile phone account when the staff member leaves the University. However:

5.12.1 a staff member may transfer their personal mobile phone number to the mobile phone account of a university-provided mobile phone, where an executive member above them in their line of management approves this transfer, and

5.12.2 where this has occurred, the staff member may later transfer the phone number back to a personal mobile phone account of their own, provided that they request the transfer before their last day of employment with the University.

5.13 When an independent contractor's engagement by the University is ending, the contractor must return any mobile device provided to them by the University, to the IT Service Desk, on or before the final day of the engagement contract.

5.14 A staff member leaving the University, unless they have been dismissed, may keep a mobile phone handset, if the handset was bought more than 24 months before their departure date.

5.14.1 Where the handset was bought 24 months or less before that staff member's departure date, they must return the handset to the IT Service Desk, on or before their final day of

employment.

5.15 When a staff member or student leaves the University, they must return to the OIT any tablet computer provided by the University.

6 USERS' OWN DEVICES

6.1 Where a user accesses a university information and communication system from their own device the University takes no responsibility for costs of using the device or damage that may come to it.

7 PHYSICAL SECURITY OF INFORMATION TECHNOLOGY

7.1 When a user leaves a university computer or device switched on, they will lock it digitally.

7.2 Users will lock away mobile devices and tablets provided by the University when not using them.

7.3 Desktop computers will not be moved to a different room without the permission of the Office of Information Technology.

7.4 Visits to secure areas such as server rooms, by staff whose role does not involve work in the area, students or people from outside the University, must be logged and the visitor must be accompanied by a staff member.

8 SOFTWARE DEVELOPMENT AND INSTALLATION

8.1 Only the Office of Information Technology (OIT) is permitted to develop or install new software for the University's enterprise information systems.

8.1.1 The OIT may, however, engage an external vendor or consultant to develop or install new software on such an information system.

8.2 The Chief Information Officer (CIO) will maintain lists of what software staff can install on types of device provided by the University.

8.2.1 Where a staff member wishes to install software that is not on the relevant list of permitted software, they will only do this after they have requested and received approval from the OIT via a request to the IT Service Desk.

8.3 To develop software to be used on university information technology infrastructure, a staff member must first have requested and received permission to do this from the OIT via a request to the IT Service Desk.

8.3.1 An academic unit that needs its staff or students to develop software for research or teaching purposes must seek approval from the OIT to do this, and must meet any conditions for the approval specified by the OIT.

9 INFORMATION TECHNOLOGY REGISTER

9.1 The Chief Information Officer will ensure that the Office of Information Technology maintains a register of the University's:

9.1.1 software and information technology licences

9.1.2 information technology infrastructure (hardware, servers and switches), and

9.1.3 information systems and their business owners.

10 BACKUP AND DISASTER RECOVERY

10.1 The Chief Information Officer will ensure that the Office of Information Technology maintains:

10.1.1 a backup plan that states how and how often each enterprise information system will be backed up, and

10.1.2 a disaster recovery plan stating processes for restoring enterprise information systems and returning them to operation if they have gone down.

11 RESPONSIBILITIES

11.1 The *Policy: Information and Information Technology* states general responsibilities of everyone who uses a university information system.

11.2 All staff

11.2.1 All staff will:

11.2.1.1 only access information they need carry out the functions of their role

11.2.1.2 where the University provides them with a mobile device for their work, meet the requirements for its use stated in section 5

11.2.1.3 ensure the physical security of computers and devices they use in their work, as set out in section 7

11.2.1.4 where they wish to install or develop software on a computer or device provided by the University:

- check whether the software is on the list of software permitted to be installed, published by the Office of Information Technology (OIT), and
- if the software is not on the list, obtain approval from the OIT before installing it.

11.3 Chief Information Officer

11.3.1 The Chief Information Officer will:

11.3.1.1 maintain the terms and conditions of access to a university information technology user account, and

11.3.1.2 ensure that the Office of Information Technology maintains:

- a register of the University's software, information technology licences and infrastructure, and information systems and their business owners, and
- backup plans and a disaster recovery plan for enterprise information systems.

11.4 Office of Information Technology

11.4.1 The Office of Information Technology will:

11.4.1.1 provide users of university information systems with access accounts appropriate to their role

11.4.1.2 terminate or change a user's access when their role changes or their relationship with the University ends

11.4.1.3 issue staff, members of the Board of Directors and, where necessary, independent consultants with mobile devices

11.4.1.4 monitor internet usage via university information technology infrastructure, and

11.4.1.5 maintain lists of software users of university computers and mobile devices are permitted to install on these.

11.5 Students

11.5.1 Students who use university information systems will:

11.5.1.1 comply with the conditions of access to their user account, and

11.5.1.2 comply with any additional conditions of access to or instructions for use of the information system set by the system owner.

12 RELATED DOCUMENTS

12.1 Mobile device request form

12.2 CIO's instructions for use of information technology web page

13 INTERPRETATION AND DEFINITIONS:

13.1 Interpretation

13.1.1 The following rules of interpretation apply to this procedure:

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

13.1.3 Should any provision in this procedure 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 procedure to the extent of the inconsistency.

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

13.1.4.1 the policy that it supports, identified in the Purpose section

13.1.4.2 closely-related policies and regulations listed in the Related policies and regulations sections

13.1.4.3 the *Code of Conduct (Staff)* and *Code of Conduct (Students)*, which include a requirement to comply with policy documents of the University, and

13.1.4.4 any other documents listed in the Related documents section.

13.1.5 Where this procedure uses:

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

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

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

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

13.1.5.5 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;

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

13.1.5.7 any gender, it includes the other genders, and

13.1.5.8 a reference to a statute, ordinance, code or other law, it includes regulation, 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.

13.2 Definitions

13.2.1 For the purpose of this procedure, the definitions in the Definitions section of the *Policy: Information and Information Technology* apply.

Version	Date of approval	Approved by	Amendment
1	2 August 2022	Vice Chancellor	Effective date – new procedure.