THE UNIVERSITY OF NOTRE DAME AUSTRALIA

Information Technology Instruction:

Access and Credentials

Effective: 23 October 2023

Audience: Employees, Students

Key words:	Cybersecurity, data, information, information security
Instruction Owner:	Chief Information Officer
Responsible Officer:	Director, IT Business Partners & Security
Review Date:	23 October 2024

Information Technology Instruction: Access and Credentials

1. Authority and force of this instruction

The *Policy: Information and Information Technology*:

- authorises the Chief Information Officer (CIO) to maintain detailed instructions for staff to ensure security of the University's information (clause 5.3.1.2), and
- requires everyone who uses a university information system or a device provided by the University to follow those instructions (clause 5.1.3), and abide by the terms and conditions of use of the system or device.

The *Procedure: Information Management* (clause 3.5.1) authorises the CIO to maintain 'terms and conditions of access to a university information technology user access account to ensure users of university information and communication systems:

- maintain their security
- maintain the security and confidentiality of the information the system contains
- use the system only for the uses for which it is intended, and
- are aware that their use of the system must comply with the relevant code of conduct.

2. Instruction

2.1. Staff receive access to information and communication systems of the University, by an automated process, for their period of employment.

2.2. Students receive access to these systems, by an automated process, in the lead-up to and during their period of enrolment at the university.

2.3. Students who have completed an award of the University will receive ongoing alumnus access to some university systems. Their student access will be changed to alumnus access by an automated process.

2.4. People other than staff or students may receive temporary access similar to that of a staff member, for purposes such as consultancy work or being an academic visitor.

2.4.1. For a person to receive this access, the manager of the relevant organisational unit must request it.

2.4.2.Information Technology will disable this access at the end of the period for which the temporary access was requested.

2.5. Where there is no other option, a user account can be created for shared use by a work team, on the request of the manager responsible for the work team.

2.6. To access information systems of the University, a user must create an access password that complies with the following requirements. Passwords:

- must have at least 12 characters
- cannot be any of the user's past 12 passwords

2.7. must not be based on anything that can be easily guessed or figured out from the user's personal information: that is, they must not:

- be based on the user’s name, date of birth, telephone numbers, family information
- have repetitive or sequential characters or numbers
- be a context-specific word such as the name of the service, the username or derivatives of these.

2.8. Passwords that are on a password blacklist maintained by IT cannot be used. These include:

- users’ previous proposed passwords that infringed the above requirements
- previously breached passwords
- dictionary words
- commonly used passwords.

2.9. A user seeking access will have 5 attempts to enter their password. After 5 unsuccessful attempts, their access will be locked and they will have to reset their password and then enter it correctly to gain access.

2.10. In their use of university information and communication systems, users must comply with the conditions of access to these systems, which are stated at the end of this instruction.

3. Conditions of access to university information and communication technology systems

To gain access, users will have to accept these conditions on first logging in as a user. Periodically thereafter they will have to re-accept them, to gain access.

Conditions of access

I understand and accept the following conditions of access to University of Notre Dame Australia information and communication systems:

Ensuring information security

- I will not share my staff number or password with another person.
- I will keep my password secure so others cannot find it out.
- I will report any possible use of my access by someone else to the IT Service Desk promptly.
- If I suspect that my password has been revealed to someone else, I will change it immediately and inform the IT service desk.

Proper use of access

- Other than for reasonable personal use (see next point), I will only use my access for purposes necessary to my research, study or work for the University.
- I may use my personal university email account and internet access for personal communications or personal transactions provided that (if I am a staff member) I do this outside my work hours or in legitimate break times (my lunch break, morning or afternoon tea break).
- I understand that the University may monitor my use of any of its information and communication systems to check whether I am using them appropriately.

Prohibited uses of access

I will not use my access to:

- communicate or use an information system in a way that breaches (as relevant to me) the University's Code of Conduct (Staff) or Code of Conduct (Students) or is non-compliant with any other policy or procedure of the University
- copy, download, store or transmit material that infringes copyright, such as music files, movies or videos
- view or download pornography, or participate in online gambling or gaming, unless I have received ethics approval to do so as part of legitimate research
- download large files such as media files unless this is necessary for my university work or studies
- operate my own business or work for an employer other than the University, other than for a work integrated learning placement or project that is part of my studies
- send spam emails or electronic chain letters, or
- break any Australian law.

Consequences of improper use of access

I understand that if I use my access improperly I may be subject to (as relevant to me) the staff disciplinary process under the Enterprise Agreement and/or the student misconduct process under the General Regulations.