INFORMATION TECHNOLOGY ACCESS AND USE POLICY

Approved by Council: 23 November 2016
Revised by Council: 28 November 2018

Related Documents

Privacy Policy

Inclusion Policy

Privacy and Data Protection Act 2014 (Vic)

Public Records Act 1973 (Vic)

Copyright Act 1968 (Cth)

1. Purpose

1.1 To establish the standards of acceptable use of the University's Information Technology (IT) and information infrastructure, and end-to-end network by authorised users.

2. Scope

2.1 The policy applies to all University and College staff, including visiting and honorary academic staff, students and visitors, and contractors across the University.

2.2 Members of the University community are permitted use of the University's IT and information infrastructure, unless explicitly denied use by the University, or under specific legislation. Authorised users are expected to use IT and the end-to-end network responsibly, efficiently, ethically, and legally. Access to, and use of, the University's IT and information infrastructure requires users to meet the obligations of this policy.

3. Definitions

3.1 "Information asset" means information that has been converted into binary digital form. In the context of the University, this includes all information stored electronically.

3.2 "Information security" means the preservation of confidentiality, integrity and availability of information assets.

3.3 "Information technology asset" means all hardware, software and connectivity access owned or managed by the University.

3.4 "User" means any person who accesses and uses University information assets. Users include University staff, students, visitors and contractors.

3.5 "Information infrastructure" includes the buildings, permanent installations, information services, fixtures, cabling, and capital equipment that comprise the underlying system by which the University holds, transmits, manages, uses, analyses, or accesses information, and carries communication.

3.6 "Integrated communication network" (ICN) means the University network infrastructure

4. Principles

4.1 Information assets are developed and made accessible for legitimate use in delivering the University's mission and authorised activites.

4.2 Unauthorised access and inappropriate use are minimised through effective controls and protection.

4.3 Users of information assets and information technology assets are aware of their responsibilities, especially in relation to privacy and security, and are informed of the rules for access and usage.

4.4 Information security is governed effectively, including identification and management of policy breaches.

5. Responsibilities of the University

5.1 The Council is responsible for ensuring that sufficient resources are available to give effect to this Policy.

5.2 The Vice-Chancellor is responsible for:

a) regular assessment of the effectiveness of this Policy

b) reporting any material breaches of this Policy to the Risk Management and Audit Committee, and, as appropriate, to the Council

c) maintaining accountabilities for information security throughout all levels of the organisation

d) establishing a Code of Practice for the use of University information technology assets through the approval and modification of Schedule 1 of this Policy

e) the assignment of responsibilities to staff members to implement this Policy through the approval and modification of Schedule 2 of this Policy

f) establishing rules for granting, reviewing, and removing access to University information technology assets through the approval and modification of Schedule 3 of this Policy.

5.3 To support the core activities of teaching and research, the Office of the Vice-Chancellor is responsible for:

a) ensuring the security, integrity, accessibility, authority and fitness of the University's IT and information infrastructure

b) providing users with relevant legal information regarding the use of IT and information infrastructure

c) ensuring software used by the University is licensed in accordance with the procurement and contracts licensing procedures, as found in the Delegations Policy

d) backing up University data in University storage infrastructure

e) optimising storage by deleting any unwanted data, subject to any requirements under the University's policy on records or archives

f) providing infrastructure networks to meet the information access needs of the University, and to enable collaboration with external, local, national and international research and education institutions

g) ensuring the physical infrastructure and networks within the University provide the basis for national and international connections, and educational and research excellence

h) identifying and managing overall risk across the University's IT and information infrastructure

i) supporting network security at a sufficient level to protect the University's information sources, electronic resources, intellectual property, and network access

j) maintaining records of information security decisions and actions

k) communicating and educating users of the principles of this policy and detailed expectations of their behavior and accountabilities.

6. Responsibilities of Users

6.1 Users of information assets must:

a) use IT and information infrastructure within the directions, limits, and obligations of University policies and procedures, and maintain an appropriate level of awareness and compliance with Schedule 1 of the Policy and applicable University policies and procedures

b) must secure and restrict access to information assets at all times including where being used outside of University premises

c) may only grant third-party access to information for legitimate business purposes and where the relationship with that third-party is approved and monitored by the University and complies with the Privacy Policy

d) must report any breaches of this Policy immediately to the Vice-Chancellor.

6.2 Any user found breaching this policy may be subject to disciplinary action in accordance with University policy and the terms of any agreement defining the user's relationship with the University.

7. Date of next review

7.1 This policy must be reviewed at least once every two years.

7.2 This policy is to be reviewed no later than 31 December 2020.

SCHEDULE 1: Code of Practice for the use of Information Technology Assets
Approved by the Vice-Chancellor: 1 January 2017
Reviewed by the Vice Chancellor: 29 November 2018

This Code of Practice for the use of Information Technology Assets supports the University of Divinity's Information Technology Access and Use Policy and applies to all users, information assets, and information technology assets (IT assets) as defined within the Policy.

The University monitors the access and use of IT assets to ensure compliance with this code of practice; this includes where IT assets are being used for personal use or where personal devices are accessing IT assets. Users are required to report any actual or suspected breaches of this code of practice by other users or themselves (even inadvertent) as per the requirements of the policy. Users found to be in breach of this code of practice are considered to be in breach of the Policy.

Access to IT assets must only be granted to authorised users who are responsible for all activity that originates from the assets themselves and user software accounts therein. This includes access to connectivity points (such as WiFi) through personal devices.

Access and stewardship of IT assets is granted for the primary purpose of advancing the University towards its mission and authorized activities. Limited personal use of IT assets, where it does not relate to University business, is permitted where it does not require a substantial expenditure of time, adversely affect the University or breach the policy or this code of practice.

Users must:

a) only use IT assets that have been allocated to them, or to which they have been temporarily granted access, by the University.

b) only access IT assets using their unique usernames and associated passwords.

c) maintain total confidentiality of their unique usernames and associated passwords.

d) ensure that physical IT assets are secure at all times both within University premises and when outside University premises.

e) advise any visitors accessing IT assets of the need to act in accordance with this Code of Practice

f) report immediately to the Office of the Vice-Chancellor if they suspect that IT assets of the University have been inappropriately accessed by third parties ('hacked') or where the confidentiality of usernames or passwords may have been compromised.

Users must not:

g) intentionally connect compromised or unapproved devices or communication equipment to the University's information infrastructure or end-to-end network;

h) intentionally attempt to breach security to access information or parts of the information infrastructure that are outside their authority;

i) allow access to the information infrastructure or end-to-end network to unauthorised users;

j) use another user's credentials, masquerade as, or represent, another user;

k) use IT, information infrastructure, or the end-to-end network to harass, threaten, defame, libel, or illegally discriminate, as defined in relevant legislation;

l) create, transmit, access, solicit, or knowingly display or store electronic material that is offensive, disrespectful, or discriminatory;

m) contravene any provision of the Copyright Act 1968 including, but not limited to, unauthorised use of copyright material, and downloading or sharing pirated content using the University's information infrastructure or end-to-end network;

n) modify or remove University information without authority to do so;

o) breach the confidentiality of others, or the University, and the confidential information of others or the University. Information is considered confidential, whether protected by the computing operating system or not, unless the owner intentionally makes that information available; and

p) not damage or destroy IT equipment used to access the information assets and end-to-end network.

SCHEDULE 2: Information and Cyber Security Staff Responsibilities

Approved by the Vice-Chancellor: 18 December 2017
Reviewed by the Vice Chancellor: 28 November 2018

Chief Financial Officer	Reports regularly to the Risk Management and Audit Committee on the status of information security at the University Reports any material breaches of this Policy to the Vice-Chancellor with recommendations for action
Director of Academic Services	Authorises the access of academic and administrative staff to University information technology assets including the student record system and learning management system. Ensures that staff and students granted access are aware of their responsibilities under this Policy. Revokes access where required under schedule 3.
Academic Systems Manager	Enables the access of academic and administrative staff to University information technology assets including the student record system and learning management system. Conducts an annual audit of users and reports results to the Director of Academic Services.
External IT support agency (Nerds on Time)	Designs Information Technology assets and implements processes for secure use. Undertakes regular information security audits or reviews, and reports results to the Chief Financial Officer. Maintains records of security frameworks and decisions.

SCHEDULE 3: Access to University information technology assets

Approved by the Vice-Chancellor: 1 January 2017
Reviewed by the Vice Chancellor: 29 November 2018

This schedule details the process for obtaining and authorities for approving access to the student record system ("TAMS"). Access to TAMS generates access to other University information technology assets including the learning management system.

Users whose access is not automatically generated must complete the IT Systems Access Form published on the University website. Completed forms must be filed securely at the Office of the Vice-Chancellor in accordance with the provisions of the University's Privacy Policy.

1. Students

Type: Student

Level: Read-only access, only for the student's own record

Access: Access is automatically generated to currently enrolled students once their enrolments have been approved by their Academic Dean or Research Coordinators and entered into University Student Record System. Access to Student Record Systems is revoked when a student ceases to be enrolled.

Support: Students should seek assistance in relation to Student Record Systems access from their College Registrar.

2. College Academic and Administrative Staff (basic access)

Type: Basic

Level: Read-only access to student records

Access: Staff must submit a completed IT Systems Access Form to their College Registrars for approval and submission to the Office of the Vice-Chancellor. Access is revoked when employment or appointment at the College has concluded.

Support: Staff should seek assistance in relation to Student Record Systems access from their College Registrar.

Training: College Registrars.

3. College Academic and Administrative Staff (advanced access)

Type: Advanced

Level: Read and write access to student records relating to the staff member's College, and read-only access to records of other students.

Access: This level of access is usually reserved for Registrars, Academic Deans, or other persons responsible for the entry of student data in Student Record Systems. Staff must submit a completed IT Systems Access Form to their College Principal for approval and submission to the Office of the Vice-Chancellor. Access is revoked when employment or appointment at the College has concluded.

Support: Registrars and Academic Deans should seek assistance in relation to Student Record Systems access from the Director of Academic Services.

Training: OVC Academic Services Manager

4. Office of the Vice-Chancellor (basic access)

Type: OVC

Level: Read and write access to all student records

Access: Office of the Vice-Chancellor staff must submit a completed IT Systems Access Form to the Academic Systems Manager for approval. Access is revoked when employment or appointment at the Office of the Vice-Chancellor has concluded.

Support: Office of the Vice-Chancellor staff should seek assistance in relation to Student Record Systems access from the Director of Academic Services.

Training: OVC Academic Services Manager.

5. Office of the Vice-Chancellor (administrator access)

Type: Administrator

Level: System administrator access

Access: Office of the Vice-Chancellor staff must submit a completed IT Systems Access Form to the Academic Systems Manager for review and recommendation to the Vice-Chancellor. System administrator access may only be granted by the Vice-Chancellor. Access is revoked when employment or appointment at the Office of the Vice-Chancellor has concluded.

Support: Office of the Vice-Chancellor staff should seek assistance in relation to Student Record Systems access from the Director of Academic Services.

Training: Director of Academic Services.

6. Suspension of access

6.1 The Vice-Chancellor may authorise the suspension of any user's access to Student Record Systems, or the reduction of the level of any user's access to Student Record Systems, for a period of up to 14 days where reasonable evidence exists to indicate that any of the following circumstances apply:

a) the user has breached the University's Information and Cyber Security Policy or its Code of Practice;

b) the user has breached the University's Privacy Policy;

c) the user is subject to disciplinary proceedings by the University;

d) the user has repeatedly entered information inaccurately and has been cautioned in writing that further inaccurate entry of information may lead to suspension of access.

6.2 The Vice-Chancellor must inform the user and the user's College Principal or Supervisor of the suspension or reduction, the reason for the suspension or reduction, and what action is required, if any, for the resumption of access.