Acceptable Use of Information Technology Resources - Governing Policy

/explore/policies-and-procedures/acceptable-use-of-information-technology-resources-governing-policy

Overview

Information technology has the ability to improve instructional systems, information systems, and communications services for staff and students in support of the University's academic programmes, research endeavours and administrative services. The University's strategic plan and operational plans direct how computing equipment, networks, systems and software (hereinafter referred to as information technology resources) shall be employed. Staff, students and other authorised users of these resources (hereinafter referred to as clients) as users of information technology resources are expected to exercise responsibility; use resources ethically; respect the rights and privacy of others; and operate within the laws of the State and Commonwealth, and the statutes, rules and policies of the University.

This policy has been created so that the University's clients, as users of information technology resources, have an understanding of the University's commitment as well as their own responsibilities, duties, and obligations.

1. Policy statement

1.1.1 The University provides information technology resources that are consistent with the mission and goals of the University. Specifically, services are provided for legitimate University purposes including approved teaching, research and administrative functions.

1.2 Free and open usage

1.2.1 The University's information technology environment is dynamic, characterised by openness, creativity and free sharing of information, to the greater benefit of universities generally. This policy shall respect this environment and inhibit these characteristics only when necessary to protect the essential interests of the University.

1.3 Authorised usage

1.3.1 The University shall determine who has access to available information technology resources. Staff may be authorised to access resources required to perform their duties. Students may be authorised to access services for academic purposes relating to their course of study at the University. Persons other than staff and students may be provided access to use information technology resources under special circumstances subject to appropriate authorisation and indemnities.

1.3.2 The playing of unauthorised games on University computing facilities is prohibited.

1.3.3 Clients are responsible for their own accounts and are permitted to access only those resources for which they have been authorised. No client may use any other client's authorisation to access any system, nor allow any other person to use his or her authorisation to access any system.

1.3.4 The University may withdraw access from any client who abuses privileges assigned to them.

1.4 Management of services

APPROVAL AUTHORITY
Council

RESPONSIBLE OFFICER
Deputy Vice-Chancellor (Academic)

DESIGNATED OFFICER
Director, Information Technology

FIRST APPROVED
3 February 1998

LAST AMENDED
31 January 2017

EFFECTIVE START DATE
10 September 2009

REVIEW DATE
1 December 2018

STATUS
Active

RELATED DOCUMENTS
Adopting Cloud-based Services - Procedures
Anti-Discrimination and Freedom from Bullying and Harassment (Staff) - Governing Policy
Anti-Discrimination and Freedom from Bullying and Harassment (Students) - Governing Policy
Anti-Discrimination and Freedom from Bullying and Harassment (Students) - Procedures
Conversion to a Fixed-term Pre-Retirement Contract - Procedures
Copyright - Managerial Policy
Copyright - Procedures
Copyright Infringement/Takedown Notice - Procedures
Electronic Mail - Managerial Policy
ICT Security - Managerial Policy
Information System Operations - Procedures
Intellectual Property - Governing Policy
Sexual Harassment Prevention (Students) - Governing Policy
Social Media - Managerial Policy
Software - Governing Policy
Student Conduct - Governing Policy
Student General Misconduct - Procedures

RELATED LEGISLATION / STANDARDS
Right to Information Act 2009 (Qld)
Public Records Act 2002 (Qld)
USC Student Charter

1.4.1 The University accepts responsibility for the maintenance of its information technology resources to standards of acceptable reliability and security; and for the provision of instructional materials and training courses to enable all staff and students to use these resources efficiently. However, those responsibilities must be managed within finite resources. The University may limit services and non-essential use where this impacts on costs or standards of performance, or implement operational procedures to encourage a rational use of resources.

1.5 Standard desktop computing environment

1.5.1 A standard suite of desktop applications software is adopted and provides benefits to the University community in the form of improved communications, training materials, and technical support services for clients with workstation connections to the campus network.

1.6 Information privacy

1.6.1 The University recognises the right to privacy of client files and communications. However, the University reserves the right to access files when necessary for the maintenance and security of information systems. Authorised personnel may examine files and directories where it is necessary to determine the ownership or recipient of lost or misdirected files, and also where the University has information or evidence that:

- system integrity is threatened
- security is compromised
- an activity has a detrimental impact on the quality of service to other clients
- the system is being used for purposes which are prohibited under University policies
- the system is being used for unlawful purposes

1.7 Network integrity

1.7.1 The campus computer network is a key element of the electronic based services that support the academic programmes and administrative operations. Hardware is connected to the network only in accordance with the University's building and information and communications technology (ICT) standards.

1.7.2 Any form of unauthorised experimentation with the campus network is prohibited, eg unauthorised installation of hardware or network software; physical interference with hardware, network connections, or cabling, etc.

1.8 Use of University property

1.8.1 The University's information technology resources, as with other University resources, shall be used only for legitimate University purposes for which the client is authorised.

1.8.2 Only incidental personal use of the University's information technology resources is permitted. Any such use must not violate any laws of the State and Commonwealth, any licences or agreements, or any rules or policies of the University.

1.9 Responsibility with regard to Australian laws, University policies and contracts between the University and external agencies

1.9.1 The University has obligations relating to intellectual property, copyright, sexual and gender-based harassment, and racial discrimination and harassment as defined by law, and in its own policies. The University expects that clients of its information technology resources shall exercise their responsibilities in this area.

1.9.2 Clients should familiarise themselves with University statutes, rules, and policies including, but not limited to those related policies identified above in this policy.

1.9.3 Clients must not use the University's information technology resources to act fraudulently in any way, e.g., falsely attributing the source of any material to another person.

1.9.4 The University has certain contractual and licensing obligations relating to the use of its information technology resources that constrain the way facilities may be used. Where there is any doubt, clients should familiarise themselves with any constraints detailed in the licence agreement. If in doubt, clients shall seek advice from the Asset Systems Specialist, Information Technology Services.

1.10 Defamation, harassment and other abusive behaviour

1.10.1 No client shall, under any circumstances, use the University's information technology resources for the purpose of defaming or slandering any individual or organisation. Information technology resources shall not be used in any way such that a reasonable individual may consider it to be harassing, abusive or obscene behaviour.

1.11 Internet access

1.11.1 Clients may not use the University’s systems to access or download material from the internet, nor use the internet in any other manner that in accordance with University policy is inappropriate, is illegal or which jeopardises security.

1.12 Illicit material

1.12.1 No client shall, under any circumstances use the University's information technology resources to access, transfer, or store illicit material. Resources shall be used only for legitimate University purposes for which they are provided.

1.12.2 The University cannot protect individuals against the existence or receipt of materials that they may find offensive. However the University may initiate appropriate action against the originator of the material if they have violated University policies or the law.

1.13 Account security

1.13.1 The primary means of security for the University's information technology resources is through the allocation of individual computer accounts and access passwords. It is every client's responsibility to ensure that:

- passwords are selected carefully
- computer workstations are kept physically secure, eg staff offices shall be secured when unoccupied, computer laboratory security measures are not circumvented
- passwords and computer accounts are not shared with other persons

1.13.2 No client shall, under any circumstances take any action that would or might lead to circumventing or compromising security of any of the University's information technology resources.

1.14 Interference with other clients

1.14.1 No client shall, under any circumstances, take any action to deny or impair access to, or effective use of, any information technology resource by any other authorised client, eg unauthorised moving of equipment; unauthorised interference with network connections or configurations, unauthorised installation or use of software on shared computers or other networked facilities, etc.

1.14.2 The promulgation of software viruses or similar contaminant software is expressly forbidden.

1.15 Electronic communications

1.15.1 Facilities for electronic communications (such as electronic mail, portal announcements, discussion forums and electronic notices) are provided for general use consistent with this and other University policies. Clients are responsible for the use of their account and the electronic messages that are sent from their account. Clients shall familiarise themselves with the University's policies, regulations, and procedures associated with the use of electronic communications.

1.16 Knowledge of breach of policy

1.16.1 Any breaches of this policy, by any individual, should be brought to the attention of Information Technology Services.

1.17 Disciplinary action

1.17.1 Breaches of this policy shall be treated as misconduct or serious misconduct and are dealt with under relevant University policy including the Staff Code of Conduct – Governing Policy, and the Student Conduct - Governing Policy. The University reserves the right to restrict access by an individual to information technology resources when faced with evidence of a breach of University policies or law. Breaches that violate State or Commonwealth law shall be reported to the appropriate authorities.

END