UNIVERSITY OF THE SUNSHINE COAST

POLICY ON THE ACCEPTABLE USE
OF INFORMATION TECHNOLOGY RESOURCES

Introduction
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 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 and students (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.

Each member of staff is provided with convenient access to a computer workstation networked to a wide variety of electronically based services available on campus, and other services accessible across the Internet. Similarly, students are provided with computer laboratories that deliver educational services. The University authorises staff and students to access information technology resources depending upon their need. The University reserves the right to withdraw access to any client with a previous history of offence or where evidence suggests that the client has violated University statutes, rules, and policies or the law.

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.

Policy Statement
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.

Free and open usage
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.

Authorised usage
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.

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.

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

Management of services
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.

Standard office computing environment
A standard suite of office 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.

Information privacy
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

The University can not 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.

Disciplinary action
Breaches of this policy shall be treated as misconduct and are dealt with under relevant University statutes, rules, and policies including the Code of Conduct, and the Student Conduct and Discipline Statute. 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.

Network integrity
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 telecommunications standards.

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

Use of University property
The University's information technology resources, as with other University resources, shall be used only for legitimate University purposes.

Staff should limit the use the University's information technology resources for incidental purposes.

Students should limit the use the University's information technology resources to purposes that directly relate to their studies.

Expression of personal views
During electronic correspondence or discussion, it must be recognised that personal views may be misconstrued to be representative of the University's position. Where the client does not have authority such correspondence must remove any such ambiguity.

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

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.

Clients should familiarise themselves with University statutes, rules, and policies including, but not limited to, the Code of Conduct, the Student Conduct and Discipline Statute, all harassment policies, and the Intellectual Property policy.

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.

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 Manager, Information Technology Services.

Defamation, harassment and other abusive behaviour

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.

Illicit Material

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.

Security

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 and not shared with other persons
- computer workstations are kept physically secure, e.g., staff offices shall be secured when unoccupied, computer laboratory security measures shall not be circumvented
- computer accounts are not shared with other persons

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.

Interference with other clients

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, e.g., 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.

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

Electronic communications

Facilities for electronic communications (such as electronic mail, bulletin boards, list servers and news) 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.

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

Acknowledgements
The information contained in this document have been derived from a variety of sources including the policies of other higher education institutions.

ITrespol.doc