INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

Introduction

This policy applies to all clients/users of ICT resources and ICT equipment owned, leased, or rented by the University of Fiji. It also applies to any person connecting personal equipment to the University network from any location. This includes, but is not limited to:

- All students;
- Academic, visiting academic and non-academic staff;
- Guests of University staff; and
- External individuals or organisations.

ICT equipment includes, but is not limited to:

- Wireless access cards, network interfaces and dialup modems;
- Desktop, notebook, mobile devices and personal digital equipment;
- Peripheral devices such as printers, scanners;
- Servers; and
- Networking equipment and communications networks used to link these components together and to the Internet.

As a condition of using the University of Fiji's ICT resources, the client/user agrees to comply with all copyright and other intellectual property laws and agreements. The client/user also agrees not to violate any civil or criminal laws in using the system.

Furthermore, client/user agrees to indemnify and protect the University (and its representatives) from any claim, damage or cost related to their use of the University's ICT resources. Use of ICT facilities is at all times subject to the conditions and constraints relating to their use in terms of University security, privacy, copyright, confidentiality policies, standards, and guidelines.

Unauthorised Use

i. The client/user agrees not to share passwords that are provided for access to University services.

ii. The client/user agrees not to use a computer account that does not belong to them.

iii. The client/user agrees to refrain from any activity that intentionally interferes with a computer's operating system or its logging and security systems, or that may cause such effects.

iv. The client/user shall be sensitive to the public nature of computer systems and refrain from transmitting, posting, or otherwise displaying material that is threatening, obscene, discriminating, harassing or defamatory.

v. The client/user agrees not to make copies of, or distribute, software the University owns or uses under license, unless permission to copy has been specifically granted by the owner of the software or the owner of the license. If the client/user is in doubt as to whether they have permission to copy software, assume the negative.

vi. The client/user agrees not to create, alter or delete any electronic information contained in any system associated with University ICT resources that is not part of their own work.

vii. The client/user shall not use University of Fiji's ICT resources as a means of obtaining unauthorised access to any other computing systems.

viii. The client/user agrees not to intentionally access, download, store, or distribute material of a pornographic nature other than with the approval from an authorised University Officer for research related purposes.

The client/user agrees not to perform any monitoring, scanning or "sniffing" of the University ICT network unless authorised by the Manager Information Technology Services

Unauthorised Personal Use

Unauthorised use of Information Communication Technology includes, but is not limited to:

i. Infringing the copyright or other intellectual property right of the University or third parties.

ii. Scanning and/or printing resources protected by copyright.

iii. Disrupting communication and information devices through such means as mass emailing or transmitting files which place an unnecessary burden on the University resources.

iv. Disrupting or interfering with the use of Information Communication Technology.

v. Effecting security breaches of network communication. Security breaches include, but are not limited to, accessing data of which the client/user is not an intended recipient, and logging in to a server or account that the client is not authorised to access.

vi. Executing any form of unauthorised network monitoring.

vii. Circumventing user authentication or security of any host, network, or account.

viii. Without authority, destroying, altering, dismantling, disfiguring, preventing rightful access to, or otherwise interfering with, the integrity of Information Communication Technology.

ix. Accessing offensive internet sites.

x. Storing of non-academic related material in the network drive share allocated.

b) Users shall not use the internet or email access to:

i. Download, distribute, store or display pornographic and other offensive graphics, images or statements, or other material obtained from offensive internet sites.

ii. Download, distribute, store or display material that could cause offence to others (for example, offensive material based on sex, gender, ethnicity or religious and political beliefs).

iii. Download and store illegal music, videos and software.

iv. Download large amounts of material for personal use.

v. Download information for external organisations or the general public, without authorisation.

vi. Distribute chain letters.

vii. Distribute defamatory, obscene, offensive or harassing messages.

viii. Distribute confidential information without authority.

ix. Distribute private or personal information about other people without authorisation.

x. Distribute messages anonymously, using a false identity or using another person’s user or email details.

Malware (Virus and Spyware)

i. Scan any removable media (USB flash drives, External hard-disks etc.) prior to using them or copying any program files contained on removable media to the University computers.

ii. Electronic mail messages and Internet file transfers may contain files that could potentially carry malware. Scan these files prior to using them on the computer.

iii. If the user's computer is infected or it is suspected that the computer may be infected by malware, contact the IT Services helpdesk immediately so that measures can be taken to remove the malware and identify any other affected computers and storage media.

Violations

i. Any suspected violations should be reported to the IT Services office immediately.

ii. Violation of this policy may result in fines and suspension of user's ICT services and may also lead to disciplinary actions by the University.

Using Internet Dongle and Pocket Wifi – Creating

Back-doors

i. Connecting an Internet Dongle or a Pocket Wifi to user's computer while user is connected to the University computer network is prohibited.

ii. The client/user must seek assistance from IT Services to make sure they are disconnected from the University computer network to avoid creating a back-door to the University Network.

Intellectual Property

i. Any software or system produced or developed while being employed by the University renders that product or software or programme with all source code an intellectual property of the University of Fiji.

ii. All use and distribution will be copyrighted by the University.

Passwords

i. Any password for any given system while being employed by the University renders that password an intellectual property of the University of Fiji.

ii. The University has the legal right to demand retrieval of that password when required from the staff member.

Vandalism and Theft

Vandalism and theft of computer gadgets such as keyboards, mouses, etc, are prohibited and will lead to disciplinary actions by the University.