ICT User Policies

Policy ID	**ICT010410**
Prepared by	**ICT Department**
Approved by	DICT
Date Issued	**1st June 2010**
Revision Date	**1st May 2013**

Contents

Section 1: Overview and Purpose of this Policy

1.1 Overview

The Fiji National University has a large investment in computing resources and has encouraged the University community to use these resources effectively to share information and knowledge in support of the University's mission of education, research, public service and to conduct the University's administration. The computer facilities are a shared system made available to promote a learning atmosphere for the University, create a sense of commitment to the local and global community and assist in preparation for living in a complex technological society. The network infrastructure, access to the Internet and online resources, powerful servers, and an increasing number of personal computers are assets in which we may take pride. Their value increases the more we take advantage of them. Using these resources in a responsible manner will protect this investment.

The University supports freedom of expression and an open environment for scholarly research. The contents of the Fiji National University ICT policy must, however, comply with other University guidelines, as well as the local laws. This document is not meant to be a comprehensive list of what is allowed and not allowed, but a guide to ensure that computing resources are used ethically and responsibly within the university community. Effective security is a team effort involving the participation and support of every University employee and student and computer user. Use of FNU's ICT Systems, when carried out on a privately owned computer that is not managed or maintained by FNU is also governed by this Policy. ***It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.***

Changes to this document may be made as new situations arise and shall reflect changes in policies and procedures.

1.2 Purpose

The purpose of this ICT policy as a whole is:

- To ensure that the ICT systems are used for its intended purposes
- To define acceptable use of systems and use of university data
- To follow government guidelines and applicable laws
- To protect the university from any possible litigation
- To establish processes for addressing policy violations and sanctions for violators

1.3 Definitions

***Authorised User*: A** university employee, student, or other individual affiliated with the University who has been granted authorisation to use a specific electronic resource.

Backup: To create a copy of critical files to minimize the loss of data in the event of a system failure.

ICT Department: The University department responsible for the purchasing, management, and support of all computer, network, and telecommunications systems on campus.

ICT Systems: These are the computers, terminals, printers, networks, online and offline storage media and related equipment, software and data files that are owned, managed or maintained by FNU.

Electronic Resource: Material in digital format which requires a computer device for use.

Email: Electronic Mail. Electronic messages sent from one person to another via electronic communication systems.

Employee: A person hired by the Fiji National University, whose primary role is to work for wages and salary.

Encryption: A security method used to transform data from its original form into a difficult to interpret format in order to prevent any but the intended recipient from reading that data.

Firewall: An access control device that acts as a barrier between two or more segments of a computer network, used to protect internal networks from unauthorised users or processes of other networks.

Internet: Global system of interconnected computers and computer networks. The computers and networks are owned and maintained separately by a host of organisations, government agencies, companies, and colleges and exist outside the FNU network.

Intranet: A private network for communication and information that is only accessible to authorised users within the university.

Institutional Purposes: Broadly defined as legitimate items directly related to the mission of the University.

Logon: *see "Username"*

Mobile Computing: the ability to use technology in a non-fixed or non-static environment or location, via a portable computing or communication device such as a laptop, tablet, PDA, or cell phone.

Password: A string of characters known only to the user that serves as authentication of a person's identity. Passwords may be used to grant, or deny, access to information or resources. Access to systems or information is usually granted by a combination of Username and Password.

Personal Information: Information related to a person's private life or concerns, recorded in any form, by which individuals can be identified. Personal information can include: full name, address, telephone number, passport number, driving license number, or FNPF number

Personal Files: Any type of record, document, or file that is of a personal nature and does not relate to the University or University business.

Privileged Information: Information confined to an exclusive or chosen group of users. Privileged information is not considered common knowledge, or has not been cleared for release to others outside the group.

Reasonable Efforts: Efforts based on known statements, events, or conditions. Reasonable efforts are defined as being within common sense, known best practices, or logical actions.

Remote Access: The ability to obtain access to an IT resource or the FNU network from a location other than a physical campus of the Fiji National University, or via a system or device not owned by the Fiji National University.

Security: Measures taken as to ensure a reliable computing platform free from the risk of loss.

Server: A system or computer program that provides information or services to other programs or devices.

Spam: Unauthorized and/or unsolicited mass electronic mailings.

Student: Person who is enrolled for study, as their primary role, at the Fiji National University.

System Administrator: ICT staff who oversee the day-to-day operation of the system and are authorised to determine who is permitted access to particular ICT resources.

TCP/IP: Transmission control protocol/Internet Protocol. This is a combined set of communication protocols that are used to perform data transfers between computers. These protocols are used to communicate over the Internet

User: Any individual who uses, logs in, attempt to use, or attempts to log into a system, whether by direct connection (modem or network) or across one or more networks.

UserID: *see "Username"*

Username: Also referred to as "logon" or "userID". A unique string of characters used to identify a specific user **in a multi-user environment. Access to systems or information is usually granted by a**

combination of Username and Password.

Wireless Network: A network utilizing radio waves to transmit data as opposed to physical wired connections. Common terms used to describe a wireless network include Wi-Fi, WLAN, or 802.11.

Webmaster: Person responsible for designing, managing, maintaining, and updating the website and web server.

Section 2: General Acceptable Use Policy

2.1 General Policies

This Policy applies to all Users of ICT Systems, including but not limited to University students and staff (both temporary and permanent). It applies to the use of all ICT Systems. These include systems, networks, student support facilities and all facilities administered by the ICT Department, as well as those administered by individual colleges, departments, University laboratories, and other University-based entities.

The University endeavours to maintain an environment free of harassment and sensitive to the diversity of its Students and staff. The University, therefore, prohibits the use of computers and email in ways that are disruptive or offensive to others and/or harmful to morale.

2.2 User Account Activation / Termination

Email Accounts will only be created on the endorsement from the Human Resources (HR) Department.

All employees of FNU are entitled to an e-mail account. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:

- Associated individuals- visiting fellows, guest lecturers, honorary research associates.
- Consultants

Applications for all these accounts must be submitted in writing/via HR Department using the form

User Email/Internet Application form (ICT 02410) and send to

ICT Helpdesk at **Samabula or email to *ICTHelpdesk*@fnu.ac.fj**

All terms, conditions, and restrictions governing e-mail use must be in a written and signed agreement in ***User Email/Internet Application form (ICT 02410). ICT Forms are available from the Z drive, ICT Forms.***

E-mail access will be ***terminated*** when the employee or third party terminates their association with FNU or proceeds on long term absence such as, suspension. This is done on the ***advice of the Human***

Resources Manager to the ICT Department. FNU is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

2.3 Data (Record) Retention

All electronic records that would normally be saved if they were paper documents should be retained on the same basis. Individual users are ultimately responsible for backing up their data files using the H and Shared drives.

2.4 Sending Messages to All Users

The ***Public Relations Officer*** under the Vice Chancellor's Office will be authorised to send messages to ***"All Users" only***.

- Staff or Respective office (s) who need to disseminate information such as important updates, newsletters, circulars, general information and notices of events to all staff, must seek approval from their Deans or Directors first and then send their Approved message to the Public Relations Office for dissemination to all staff. The VC may approve others as per situation and need.
- Deans have the privilege to send emails to all staff in their respective Colleges and distribution groups (mailing lists) as per respective schools.
- Similarly Heads of Schools and or Departments have similar privileges to their respective distribution groups.

2.5 Right to Monitor and Confidentiality

The e-mail systems and services used at FNU are owned by the University, and are therefore its property. This gives FNU the right to monitor any and all e-mail traffic passing through its e-mail system. In addition, backup copies of e-mail messages may exist, despite end-user deletion, in compliance with FNU records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss. If FNU discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due processes. All reasonable efforts will be made to notify an employee if his or her e-mail records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.

The authority to inspect the machines, servers and files resides with the Vice Chancellor through the ICT Department. Disclosure to any external organisation will only be considered on production of a legal authority.

For security and network maintenance purposes, authorized individuals or System Administrators may monitor equipment, systems, and network traffic at any time, per established monitoring and audit procedures. For purposes of system maintenance all data and transmissions may be monitored, analysed and viewed. The University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.6 Security

All users are expected to keep authorisation codes secure. Passwords should not be shared with others and should be changed frequently. Users are responsible for all actions taken using their password.

The Fiji National University cannot provide a system that allows users to store confidential information. For purposes of system maintenance networked files may be viewed. Users can assume networked information is free from censorship if the user complies with acceptable use and ICT policies. If at all possible, users will be notified if stored network information must be removed. Confidentiality will be maintained when Acceptable Use policies are followed. Users must be aware that electronic media is never 100% secure.

Stored information may be removed for reasons that include but are not limited to the following:

- The stored material was obtained illegally.
- The stored information endangers the integrity of the system.
- The user has used excessive storage system space.
- The stored information is in violation of local laws.
- The stored information is inconsistent with the policies of The Fiji National University.

All media is susceptible to viruses and other types of malware. Therefore, users must make reasonable efforts to be sure their media is free from these types of destructive programs before using in any FNU computing facility.

2.7 Loss of Damage to personal property

The Fiji National University is not responsible for any loss or damage to anyone's personal property including hardware, software or property of a mixed nature as a result of the use of the FNU's ICT facilities. The Fiji National University resources are for institutional purposes only.

2.8 Enforcement

Users violating these polices will be subject to disciplinary action, up to and including dismissal, and will be reported to proper legal authorities as required by the situation.

At a minimum, access to network and computer resources will be revoked.

Section3: Unacceptable Use

The following activities are deemed Unacceptable Use and are prohibited:

- Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation,

soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).

- Email signatures must not carry embedded messages. Commercial, religious, humorous, political or other content in embedded signatures may cause offence or bring the user or FNU into disrepute.

- Misuse of the Address Book - Mailing Lists and propagating messages to All Users or Distribution Groups.

- Sharing or revealing Username and password with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.

- Personal use of FNU e-mails resources. FNU does not allow personal use of FNU domain (…@fnu.ac.fj) for communication with family and friends, independent learning, and public service, as it interferes with staff productivity, pre-empt any institutional activity and unnecessarily congests the email resources. FNU prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-FNU commercial activity, political campaigning, dissemination of chain letters, religious messages, and use by non-employees.

- Use of illegal or unlicensed software

- Unauthorized network monitoring

- Copying and/or distributing commercial software without proper licensing

- Knowingly creating, executing, forwarding, or introducing any computer code designed to self-replicate, damage, or otherwise impede the performance of any computer, network device, or software

- Making fraudulent offers of products, items, or services originating from a FNU account.

- **Use of unauthorised devices.** Without specific authorisation, Users must not physically or electrically attach any additional device (such as non FNU Computer, an external disk, printer, or video system) to ICT Systems.

Section 4: Data Management

4.1 Backup Policies

4.1.1 Scope

Backup procedures and policy intent is to cover all production server-based applications and data, allowing business resumption after the loss of a single server or an entire site. Only servers managed by ICT Department are covered by this policy. Backup of material stored locally on end-user workstations is the responsibility of the user. ***For this reason, all users are strongly recommended to store copies of critical documents/files on H drives and the network share drives, and not on local drives.*** Refer to

Appendix 2 on Network Storage Device.

4.1.2 Scheduling and Retention

A complete backup of all production servers will be made at least once per week, the most recent kept on-site for file recovery and the next most recent stored off-site. Between weekly backups, incremental backups will be used daily to ensure that a complete backup from the previous night is always available. Incremental sets will be maintained for a minimum of two weeks.

Backups shall normally be performed at night and on weekends. ICT Department reserves the right to perform backups at any time, as deemed necessary by server administration.
Departments should be aware of documents that they are required to retain, and the method in which they must be stored.

4.1.3 Storage

All backup media shall be stored in a secure and environmentally controlled area. Removal from this secure area shall only take place for the purpose of using the media to perform a restoration, or moving backup sets to a designated off-site location. Access to this material shall be limited to ICT staff with a direct job responsibility requiring access.

4.1.4 Restoration

Servers requiring recovery from equipment failure or other catastrophic loss shall have the highest priority in restoration efforts. Requests for the restoration of individual files shall be handled as time allows.

4.1.5 Servers residing off-campus

Hosted applications and servers that do not reside on campus may not fall within the University's ability to directly protect via in-house backup procedures. However, the University must take steps to ensure that business critical information is protected from disaster, regardless of physical location. Backup and restoration policies and procedures for all hosted applications will be documented and kept on file with the appropriate department. Before entering into an agreement for any hosted application, it must be determined that backup procedures are adequate for the type of service hosted.

4.2 Information handling

4.2.1 Care and Handling of External Information

External information is be defined as any information collected, bought, or given by a source outside the

university. Many times this information comes with copyright or confidentiality agreements that dictate how the information is used. The university will adhere to any such agreements accompanying this information

4.2.2 Care and Handling of Internal Information

Internal Information is defined as any information collected and maintained by the University. The FNU is the owner of this information. Respective managers are responsible for handling the appropriate information.

4.2.3 Data Misuse

Data misuse is defined as using university-owned data (either unintentionally or deliberately) in a manner inconsistent with university policy, or local laws. Examples of data misuse include:

- Obtaining or attempting to obtain access to data not within the scope of one's University job responsibilities
- Downloading or exporting centrally held information into non-approved databases or personally owned equipment
- Using University data for personal benefit
- Releasing information in an inappropriate manner
- Using information inaccurately, conflicting with published, sanctioned University information and/or statistics

Section 5: Access Policies

5.1 Username and Password Policies

5.1.1 Employee Responsibilities:

Employees will be assigned a FNU account that allows use of certain FNU computing resources. Accounts will be designated by a username (User ID) and protected by a confidential password known only to the employee.

Employees are required to enter their username and password in order to use FNU computing resources.

Passwords must be changed as determined at the domain level. Users will be reminded to change their password days in advance. If users do not change their password by the end of this time, the account will be locked and they will not be able to log in until a password administrator unlocks it.

Employees should avoid writing their password. If they must do so, they are responsible for ensuring that no one else has access to the written password. Users shall never write both the username and password together.

Users are responsible for protecting user identification and passwords. If it is believed that someone else knows a user's password, or is using an account other than their own, the password should immediately be changed and ICT Helpdesk notified.

Users **must not** share their password with anyone, or log in and allow another user to work using their personal User ID and password. If there is need to grant access to an outside user, that user must follow appropriate procedures to apply for access.

If a password is forgotten or needs to be reset, the request must then contact the ICT Helpdesk. Passwords will not be sent via mail or email, or given to others.

5.1.2. Password Requirements

A network password is the key to access most systems on campus. All FNU employees and users are expected to keep ALL system passwords private. Our security policy requires the following:

- It must have a minimum of eight (8) characters
- It must not contain all or part of the user's account name
- It must contain characters from at least three of the following four categories:

1. English Uppercase characters (A through Z)
2. English Lowercase characters (a through z)
3. At least one number (0-9)
4. Non-alphanumeric characters (example:!, $, #, %,^)

In addition, we strongly recommend:

- It should contain both lower and upper case letters (passwords are case-sensitive)
- It should contain *at least* one special character (@, #, {,},$,%, etc.
- Never use a person's name or any word that could be found in the dictionary. Breaking up words with special characters or numbers is an easy way to avoid this.
- Do not use the same passwords for work as you do for personal use

5.2 Access Audits

ICT Department may routinely audit access to university computing resources and reserves the right to

temporarily disable questionable access. Department heads are responsible for periodically reviewing access to their information and must notify ICT if access should be revoked or levels changed.

Section 6: Internet Policies

6.1 Internet Security Policy

Internet Users shall be aware that as they access Internet resources, they will be associated with the University through the mechanisms of the TCP/IP protocols. Therefore, users shall access resources in accordance with their job description.

While online, users shall be cautious as to what they disclose to others. Users shall remember that email and internet transmissions are not private information. Anything sent could possibly be read by individuals other than the intended recipient. Users shall not transmit any information that may be damaging to the organization or themselves. Privileged and private information, as covered in other university policies, shall not be transmitted without proper precautions. Users should exercise similar care when transmitting personal data.

Section 7 Email Policies

The purpose of this policy is to outline the security of email and state FNU and User responsibilities in regard to email systems and content.

7.1 Email definitions and purpose

The campus faculty and staff e-mail system is provided as a means of communication of FNU-related business. Electronic data (including backup copies) stored, maintained, or using FNU equipment is the property of FNU, not the user. Electronic messages should follow the same standards expected in written communication, and should adhere to the ICT Policies as well as any other applicable FNU policy.

Email is the equivalent of an Internet “postcard”, and cannot be guaranteed private. Users should be aware that emails could be received, forwarded, intercepted, printed, or saved by people other than the intended recipient. The University reserves the right to monitor content and usage for maintenance, operational, auditing, security, or investigation-related reasons.

7.2 Email Antivirus Protection

ICT staff members are responsible for creating and maintaining procedures for preventing and handling infected email messages. Email that has been found to be infected with a virus, worm, Trojan horse, or contains another executable item that could pose a threat to security will not be delivered to the user. Known infected email will be removed from the delivery system. If a virus outbreak is suspected, email service may be interrupted without notice. Refer to Appendix 1 on Antivirus Policy

7.3 Mail Box Size Limits

Mailbox sizes will be limited as appropriate based on current mail server storage capacity. Email messages sent to and from outside FNU shall not exceed limits set by the email administrator.

Section 8: Software Compliance

8.1 Software Guidelines

It is the policy of the Fiji National University to respect all computer software copyrights and to adhere to the terms of all software licenses to which FNU is a party. The University shall take all steps necessary to prohibit users from duplicating any licensed software or related documentation for use either on FNU premises or elsewhere, unless expressly authorized to do so by the licensor.

8.2 Acquisition of Software

All software to be acquired by the University must be justified by the Users and appropriate approval sought. Software may not be purchased using business credit cards, petty cash, travel, or entertainment budgets. Software acquisition channels are restricted to ensure that FNU has a complete record of all software that has been purchased for FNU, such that FNU can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

8.3 Software Installation

After the registration requirements have been met, the software shall be installed by a member of ICT staff. Once installed, the original media shall be kept in a storage area maintained by ICT. User manuals, if provided, shall either reside with the user or reside with the ICT (dependent on the situation).

8.4 Home Computers

FNU computers are University-owned assets and must be kept both software-legal and virus free. Only software purchased through the procedures outlined above may be used on FNU machines. Users are not permitted to bring software from home and load it onto FNU computers. Generally, FNU-owned software cannot be taken home and loaded on a user's home computer. However, some software packages allow home use in some circumstances. If a user needs to use software at home, he/she should consult with ICT Services to determine appropriate licensing.

Section 9: Telecommunications

9.1 Phone Usage

Employees will be given phones and voicemail where and when available as necessary for conducting University business. Personal use of these phones is not encouraged.

Departments and Colleges shall monitor their monthly usage of the phones and verify the bills received. Refer to the ICT –Telephone, Mobile Phone and Wireless Broadband user policy document.

Section 10: -Physical Security

10.1 Purpose

The purpose of this policy is to outline the minimum physical security expected for Computing facilities and all computing equipment.

10.2 Computing Facilities

Computing facilities shall be of sufficient size with multiple exits. The areas used for servers shall have sufficient environmental controls that include temperature and humidity controls. For critical sites necessary fire protection systems shall be installed.

Sufficient access controls shall be installed to prevent unauthorised physical access to computing facilities.

10.3 Office/ Workstation / Laboratories.

All users shall be responsible for maintaining the security of their assigned workstation. Required security provisions include locking or logging off workstations when not in use, and preventing unauthorized physical access to unattended systems. Similarly Lecturers and or Laboratory Technicians shall maintain the computers in the laboratories.

11 Reporting Misuse

Allegations of misuse that may include events having actual or potential adverse effects which compromise an aspect of the computer, network or user resources, loss of confidentiality of information; a compromise of the integrity of information; misuse of service, systems or information; damage to systems and damage or loss of property or information. Users must report to the ICT Department or email the ICTHelpdesk@fnu.ac.fj, with the following information.

- Date and time of incident
- Type of incident and any other pertinent details that would assist in verifying incident
- A statement describing the impact on users, department or the network including the number of Users/departments affected.
- Contact information of submitter

12 Failure to Comply

Penalties for unacceptable use of University's ICT resources: The Director ICT responsible for the University's ICT or staff acting under authority of the Director ICT , will advise the Human Resources

Manager, who may impose the following penalties on those involved for unacceptable use of the University's ICT resources:

Two written warnings, Suspension, restriction or termination of access to some or all ICT resources for any third occurrence by a user.

Payment of commensurate compensation to the University for any loss or damage caused by unacceptable use of ICT resources.

If the unacceptable use of the ICT resource continues after suspension, restriction or termination of access to some or all of the ICT facilities, the person (staff/student) shall be subject to the University's Student Discipline Committee and/or Staff Conduct Committee procedures.

The Vice-Chancellor, upon the written advice of the Director ICT, and Director HR may summarily dismiss any student or staff involved in serious misconduct in relation to use of University's ICT resources.

Appendix 1 Anti-Virus Policy

Purpose

The purpose of this policy is to provide instructions on measures that must be taken by FNU employees to help achieve effective virus detection and prevention.

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, memory sticks, external hard drives, CD's and DVD's. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Fiji National University hereby referred to in this document as FNU, in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of FNU is to provide a computing network that is virus-free.

Scope

This policy applies to all computers that are connected to the FNU network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both FNU-owned computers and personally-owned computers attached to the FNU network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

General Policy

FNU installs Licensed copies of Antivirus software on its network. The most current available version of the anti-virus software package will be taken as the default standard.

All computers attached to the FNU network must have the FNU standard, supported anti-virus software installed. This software installed in computers will automatically be active, to perform virus checks at regular intervals, and have its virus definition files kept up to date. The user computer will update virus software automatically once logged into the FNU network.

Any activities with the intention to create and/or distribute malicious programs onto the FNU network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

If an employee receives what he/she believes to be a virus or suspects that a computer is infected with a virus, it must be reported to the ICT department immediately at ICT Helpdesk

Any virus-infected computer will be removed from the network until it is verified as virus-free.

Rules for Virus Prevention

1. Always run the standard anti-virus software provided by FNU.
2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
3. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.
4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
5. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
6. Avoid direct disk sharing with read/write access. Always scan the Memory Stick/External Hard Drives/CD-ROM/DVD-ROM for viruses before using it.
7. If instructed by ICT Help Desk to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

8. Back up critical data and systems configurations on a regular basis and store backups in a safe place.

ICT Department Responsibilities - Antivirus

The following activities are the responsibility of the FNU ICT department:

1. The ICT department is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted on the intranet.
2. The ICT department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use. The user computer will update automatically once logged into the FNU network.
3. The ICT department will apply any updates to the services it provides that are required to defend against threats from viruses.
4. The ICT department will install anti-virus software on all FNU owned and installed desktop workstations, laptops, and servers.
5. The ICT department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the ICT department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.
6. The ICT department will attempt to notify users of FNU systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated.
7. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

College, Department and Individual Responsibilities

The following activities are the responsibility of FNU colleges, departments and employees:

1. Colleges, Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.
2. All employees are responsible for taking reasonable measures to protect against virus infection.
3. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the FNU network without the express consent of the ICT department.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action.

Appendix 2 Network Storage Drives

About 'Network Drives'

Network drives are managed centrally and because they are automatically backed up by ICT Services they provide you with secure data storage. At the FNU you have access to the following network drives:

H: Home Drive (Personal Storage space for your backup)

W: Work Drive (Shared within your specific College/Department Filestore)

S: Shared Drive (Relevant Information that needs to be Shared within multiple Colleges and Departments)

Y: Photo gallery (Share photos within Departments and across FNU, to remove after a month)

Z: FNU Forms (Users can access commonly used forms)

H: drive (Personal Storage Space)

When using a home computer you will usually save your files to the computer's C: drive but on University computers you are to save to the **H: drive** because the H: drive is a network drive it has the advantage that it is available to you from any computer on campus and it is regularly backed up.

Secure	✓ Only you have access to your H: drive.
Backed up Automatically	✓ The H: drive is automatically backed up - in the event of a disaster you should be able to recover files.
Off Campus Access	✗ The H: drive is currently not available from off campus
Designed for Sharing	✗ It is not possible to share files on your H: drive but a better option is to use the W: drive.

Quota Allocations

Staff – 3GB. Increase to 4GB available on request and verification by ICT Helpdesk.

Obtaining Access

To access the H: drive

- Choose **start** > **My Computer** to display a list of drives available.
- Double-click on ***your username*** **on "\\Optimus\FNUUsers** to display the contents of the **H:** drive.

W: drive - Shared Departmental Filestore

The W: drive is a shared departmental filestore for staff to share files. Like the H: drive it is a "Network drive" and it is managed centrally by ICT Services and regularly backed up. Each department controls that can access their files stored on the W: drive and also whether they can edit, or just read them. Your Departmental IT Contact Person should be able to tell you what's already available and also help you with your use of the W: drive.

Secure	✓ Departments control access to files on the W: drive.
Backed up Automatically	✓ The W: drive is automatically backed up - in the event of a disaster you should be able to recover files.
Off Campus Access	✗ By default no access is available from off campus. ✓ A folder called **Web Access** must be created to provide access to the W: drive off campus. *(not available yet)*
Designed for Sharing	✓ Yes, this is the usual place for departments to store files that they wish to share.

Quota Allocations

The default quota allocation given to departments for the W: drive is 25GB. Space on the W: drive is limited but more quotas may be available by asking your Departmental IT Contact Person to contact the ICT Helpdesk.

Obtaining Access

To access the W: drive

- Choose **start > My Computer** to display a list of the drives available.
- Double-click on **Departments\Colleges on \\optimus\common** to list the departmental folders available on the W: drive.
- Double-click on the folder for your department.

Appendix 3 ICT Forms to Use

The following ICT Forms are available from Z drive, for staff to use when requesting services from the ICT Department.

Please not that certain forms do require senior management or HR Departments endorsement.

Forms:

1. User Email/Internet Application ICT 020410
2. Computer /Peripherals Requisition Form ICT 040510
3. End User Service Test ICT 070710
4. Flash Net ICT 080810
5. Fault Request Form ICT 030410
6. ICT Acceptable Asset ICT 030410
7. Mobile Phone Issue ICT 141010
8. Software Request ICT 060510
9. Telephone Request ICT 121010