Ndejje University

Ndejje IT Services (NIS)

ICT POLICY MANUAL

Version 1.10

Commencement Date: 1 August 2008

Category: Information and Communication Technology

CONTENTS

Information Security Policy

PURPOSE

To ensure that Information and Communication Technology (ICT) facilities, services, programs and data are protected from threats, whether internal or external, accidental or deliberate.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to the University data and voice networks.

EXCEPTIONS

The Chief Information Officer may approve exemption or partial compliance with the requirement for network infrastructure equipment to be managed by Ndejje IT Services where business, technical or operational reasons preclude full adherence.

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

Policy Framework

The University will establish policies, standards, guidelines and procedures to ensure:

- all of the University ICT facilities and services, programs and data are adequately protected against loss, misuse or abuse;
- all users are aware of their responsibilities for the security and protection of facilities, services, programs and data over which they have control and that they comply with Information Security policy, standards, guidelines and procedures, and the relevant Federal and State legislation;
- the information security architectural issues are considered in relation to existing systems and proposed acquisitions.

Confidentiality of Information

Prior to disposal of ICT equipment owned, rented, or leased by the University, information (for example, information stored on hard disks) shall be securely overwritten by authorised ICT personnel to ensure that all sensitive data and licensed software have been removed.

Network Security

The CIO shall define and publish minimum standards and specifications for protocols and devices authorised for connection to the University network.

All network infrastructure equipment shall be acquired, installed, controlled, and managed by Ndejje IT Services, including, but not restricted to, routers, switches, wireless access points, telephone modems configured to accept incoming connections, and any other equipment not defined above.

The following equipment may be connected to the University network without reference to the CIO or delegate: laptops, workstations, personal digital assistants (PDAs), mobile phones, and printers.

The University may undertake any lawful action including disconnecting devices from the network, deactivating sub-networks, or any other action required to protect the University's Information, Communication and Technology (ICT) facilities, services, programs and data and to ensure the integrity of the University network.
Users shall not disable security services, devices, or software on any University ICT facility or service, nor attempt to circumvent measures that enhance information security or adherence to copyright legislation unless explicitly authorised by the Chief Information Officer.

PROCEDURES

User Responsibilities

Effective information security is a team effort involving the participation and support of every user. It is the responsibility of all users to understand the need to conduct their activities accordingly.

NIS shall develop and periodically update explanatory materials explaining staff responsibilities in relation to information security.

A summary of University ICT policies shall be included with the material provided to new staff members.

All staff shall undertake training in relation to information security and ICT policy matters.

Compromised Equipment

Upon notification that equipment has been compromised or is behaving inappropriately, NIS Infrastructure staff shall immediately isolate the equipment from the network and advise the appropriate NIS team to liaise with the equipment's user about rectification of the issue and restoration of the equipment.

Risk Identification

Persons responsible for the management of ICT equipment and business systems shall undertake regular risk reviews of their respective ICT environments to ensure that all risks are identified and all reasonable measures are taken to prevent security breaches. The outcomes of the review shall be reported to ICT Strategy and Planning Committee.

ICT staff shall assist in maintaining the security and integrity of the University's ICT infrastructure facilities and services by promptly reporting any risks identified to the NIS Executive, including an assessment of the risk and a suggested treatment strategy.

Procedural Development

Where risk treatment strategies involve procedural changes within ICT teams, once approved, the Chief Information Officer shall require the revised procedures to be incorporated in the NIS Operational Procedures manual.

Non-compliance

Any breach of this policy will be managed in accordance with the ICT Breach Management policy.

ICT Use Policy

PURPOSE

To ensure that the members of the University community may use University Information and Communication Technology (ICT) facilities and services in an appropriate and responsible manner and to ensure that other persons do not misuse those ICT facilities and services.

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

The University shall issue a unique username and password to staff, students, and University Associates to enable the appropriate and responsible use of Information, Communication and Technology (ICT) facilities and services.

Authorised users shall use University Information and Communication Technology (ICT) facilities and services in an appropriate and responsible manner. Incidental personal use of University facilities and services is permitted. Any other use is considered to be inappropriate use and action may be taken under the University ICT Breach Management Policy (refer to Schedule A Appropriate Use of University ICT facilities and services for an overview of permitted uses).

Generic usernames (those that are not individually issued) shall only be issued under strict control procedures.

Access to these facilities and services is granted as a privilege; the University reserves the right to monitor, record and inspect electronic information and ICT-related activities; and to limit, restrict, cease, or extend access to Information and Communication Technology (ICT) facilities and services.

PROCEDURES

Usernames for Staff and University Associates

A username and password are automatically issued to each staff member and each University Associate as part of University business processes.

Usernames for Students

A username and password are automatically issued to each student as part of University business processes.

Compliance Education

The CIO shall provide examples of appropriate and inappropriate use of University ICT facilities and services. This information can be found in the Schedule to this policy.

SCHEDULE A - Appropriate Use of University ICT facilities and services

A person using Ndejje ICT facilities and services is responsible for ensuring that they comply with University ICT policies.

Appropriate use of Ndejje ICT facilities and services includes but is not limited to:

a) You shall use University ICT facilities and services in a manner which is ethical, lawful and not to the detriment of others.
b) You shall use only those University ICT facilities and services you have been authorised to use.
c) You shall only access ICT facilities and services on sites outside Ndejje with the owner's permission and in a manner consistent with the owner's conditions of use.
d) You shall actively defend your access to the University's ICT facilities and services from unauthorised use by others, including complying with the Password Policy (by keeping your password secret).
e) When using University ICT facilities and services you shall produce your Ndejje ID card if requested to do so by an authorised member of staff.
f) You shall abide by instructions given by the Chief Information Officer or by their delegate. Such instructions may be issued by notice displayed in the vicinity of ICT facilities, by letter, by electronic communication, in person or otherwise.
g) When you cease to be an enrolled student, a University Associate, or an employee of the University, your access to University ICT services and facilities will be terminated without notice. You are responsible for personal information you have stored on University ICT services and facilities and must make arrangements for its retention and/or removal as appropriate prior to leaving the University. Note that University records may only be disposed of in accordance with the University Policies.
h) You may use University facilities and services for incidental personal use (e.g. occasional emails and web browsing during work breaks) provided that such use does not interfere with University business operations, does not breach any Federal legislation, State legislation or University policy or an ICT vendor's conditions of use or licence agreement. Some examples of interference with University business operations include: disrupting ICT facilities or services; burdening the University with significant costs; or impeding one's work or other obligations to the University.

What <u>not</u> to do…

i) You shall not obstruct others in use of a Ndejje ICT facility or service to achieve the functions and objectives of the University.
j) You shall not use any account that has been created for another user without authorisation, nor shall you attempt to find out the password of another user, access or alter information, services, usernames, or passwords without authorisation.
k) You shall not attempt to subvert security measures in any way, nor use a false identity when using ICT facilities and services.
l) Without the explicit authorisation of the Chief Information Officer, you shall not possess any tools nor undertake any activities on Ndejje ICT facilities or services that could result or assist in the violation of any Ndejje policy, software licence or contract. Examples of these prohibited tools include viruses, Trojan horses, worms, password breakers, network packet observers or sniffers. Examples of prohibited activities include creating ping floods; spoofing packets; performing denial-of-service attacks; forging routing

information for malicious purposes; scanning for vulnerabilities; or other computer hacking techniques.

m) You shall not attempt to adversely interfere with the operation of any of the University's ICT facilities and services. For the purposes of this document, interfering includes wilful physical damage, wilful destruction of information, wilful interruption of normal operations, and accessing restricted areas without the permission of the Chief Information Officer.

n) You shall not wilfully waste ICT resources. For example, wasting network bandwidth by downloading or sending large amounts of material that is neither work-related nor study-related.

o) You shall not use the University's ICT facilities and services to send obscene, offensive, bogus, harassing or illegal messages.

p) You shall not use the University's ICT facilities and services for commercial purposes nor publish or circulate information about other organisations via the University's ICT facilities and services, except where these activities clearly support the business or purpose of the University.

q) You shall not use the University's ICT facilities and services in a way that breaches any University policy.

r) You shall not intentionally create, view, transmit, distribute, copy or store pornography or objectionable material via University ICT facilities and services unless it can be clearly demonstrated that it is required for teaching, learning, or research purposes.

s) You shall not intentionally create, view, transmit, distribute, copy or store any information, data or material that violates State legislation. (e.g. sexually explicit material involving children, incitement to violence, torture, and bestiality). You shall also not give a person under the age of eighteen years of age access to material regarded as restricted by the (e.g. matters of sex, drug misuse or addiction, crime, cruelty, and violence).

t) You shall not attempt to conceal or erase the evidence of a breach of University ICT policy.

ICT Electronic Messaging Policy

PURPOSE

To ensure the University's electronic messaging services are used in an appropriate and responsible manner.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

The University permits users to use electronic messaging services in an appropriate and responsible manner.

A user's access to electronic messaging services shall be withdrawn:

- upon instruction by an Executive Manager, Head of School or Head of Area;
- when a staff member's employment with the University ceases;
- when a University Associate's association with the University ceases; or,
- when a student ceases to be eligible as a result of a change of enrolment status.

Records created by University staff during the course of University business are owned by the University and as such form part of Ndejje's corporate assets. Users of electronic messaging services must be aware of their responsibilities in regard to the creation, capture, retention and disposal of University records.

Where access to University records is required in support of the University's business and purposes (such as files and email stored by a staff member who is on extended leave, or is no longer associated with Ndejje), an Executive Manager may authorise NIS system administrators to grant another person access to that information. Please refer to the ICT Monitoring Policy for procedure to be followed.

PROCEDURES

Caveats in relation to Electronic Mail

Electronic mail is a public communication medium that uses a store-and-forward mechanism to pass each message through multiple servers owned by other organisations and via many communication links world-wide. It is subject to misuse by individuals and organisations worldwide, who send large numbers of unsolicited “spam” email messages to many email addresses.

As a result, the University cannot guarantee:

- The successful delivery of electronic messages travelling outside the University.
- The confidentiality of information contained in electronic messages travelling outside the University.
- That all “spam” email messages are blocked from entry to the University email system.

Limitation on Message and Attachment Size

Users shall minimise network traffic by reducing the size of large messages and attachments prior to transmission. Large files should be compressed before attaching them to the message to minimise network traffic.

Electronic documents in excess of any mail server’s maximum allowable size may automatically be barred from transmission to the intended recipient. Large documents are best made available by sending recipients a link to the document ; or in some cases, writing it to a CD or DVD and sending it by courier.

Appropriate Use of Electronic Messaging Services

Electronic messaging users shall act in a professional and ethical manner. For example, users shall:

- maintain professional courtesies and considerations in electronic communication.
- not transmit abusive or defamatory messages.
- not transmit an electronic message that breaches legislation or contravenes University policies.
- not cause interference to other users of electronic messaging services. Examples of interference include transmission of e-mail chain letters, widespread distribution of unsolicited e-mail, junk mail, pyramid mail and the repeated sending of the same message.
- not give the impression that they are representing, giving opinion or making statements on behalf of the University, unless authorised to do so.

Non-compliance

Users who contravene this policy may be subject to the provisions of the ICT Breach Management Policy.

SCHEDULE A Maximum permissible email message sizes

The Ndejje email server will not send **or receive** any message which is greater than 20MB in size (including the message body and all attachments).

The Ndejje student email server will not send any message which is greater than 5MB in size (including the message body and all attachments).

ICT Breach Management Policy

PURPOSE

To deal with inappropriate or irresponsible use of University Information and Communication Technology (ICT) facilities and services.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

Each alleged breach shall be investigated to determine whether it was accidental or deliberate; this may determine whether any further action may be taken.

Users who are found to have breached a Ndejje ICT policy shall be subject to disciplinary processes.

Management of a breach of policy is determined by the facts of matter. Penalties will be applied in line with University misconduct processes set out in the applicable employment instruments, contract of employment or University Statute and may include:

- Suspending the user's University network access.
- Suspending the user's University external Internet access.
- Recovering internet traffic costs associated with an Internet-related breach from the user.
- Censure or reprimand.
- Withdrawal of benefit.
- Dismissal

PROCEDURES

Incident Reporting

Information systems security incidents shall be reported to the Faculty ICT manager for assessment. The Faculty shall undertake a disciplinary process in consultation with Staff Services or Student Services (as appropriate) and the CIO or delegate, using the Schedules to this policy as a guide to the appropriate course of action.

Regardless of the level at which an incident is resolved, all information security incidents must be reported by the ICT support staff via Service Desk and assigned to the group **information security** to enable University-wide capture of incidents for reporting purposes. The identity of the alleged offender must not be identified in the service call.

Breaches of policy may be referred to the Police upon the advice of the Standards and Integrity Officer and Legal and Compliance Services.

Breach Management Reporting

A quarterly management summary shall be provided to the Chief Information Officer. The names of persons who have breached ICT policy shall not be included in this report.

ICT Defence Policy

PURPOSE

To defend Information and Communication Technology (ICT) facilities and services against attacks by computer malware.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

The Chief Information Officer may approve exemption or partial compliance with this policy where technical or operational reasons preclude full adherence.

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

Approved defensive measures shall be deployed and kept up-to-date on Information and Communication Technology (ICT) equipment, facilities and services owned or leased or provided by the University in Western Australia campus locations.

PROCEDURES

Faculty managers and system administrators shall ensure that desktop computers and infrastructure equipment in their area of responsibility complies with the defensive measures defined in the NIS Internal Procedures manual.

The Chief Information Officer may approve either exemption or part-compliance with this policy where the requirements of this policy cannot be fully implemented in a particular ICT facility or service for operational reasons. When exemptions or part-compliance with this policy are approved, the details of the approval will be forwarded to ICTC for noting.

ICT Password Policy

PURPOSE

To control the risk of unauthorised access to University Information and Communication Technology (ICT) facilities and services by using single factor passwords.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

The Chief Information Officer may approve exemption or partial compliance with this policy where technical or operational reasons preclude full adherence.

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

All password controlled ICT facilities and services shall comply with the following minimum password standards:

Description	Standard
Length of password	Minimum of 8 characters
Structure – Mix of characters	At least one alphabetic and at least one non-alphabetic character
Number of unsuccessful login attempts before the username is made inaccessible automatically (locked)	5 times
Duration of lockout period	Minimum of 30 minutes
Period after which a password must be changed	180 days (every 6 months) - Users have the ability to change their own passwords at any time
Reusability of old passwords	Users will not be allowed to use a password they have used before within the last 12 months

Revealing a University password:

1. to a person outside the University is prohibited unless it has been authorised and is required to enable vendor ICT support engineers to maintain Ndejje ICT services or facilities.
2. to another University staff member is prohibited unless the password is required to enable University ICT support staff to maintain a ICT service or facility.
3. to another University student is prohibited.
4. A user shall not store a password in an insecure location.

Business Owners shall ensure that password controlled ICT services comply with the following password management principles:

- Usernames and passwords can be disabled on cessation or transfer of users.
- New or replacement passwords are sent to the user by a secure method.
- All passwords used in automated and/or unattended processes are encrypted where possible.
- When acquiring new Information and Communication Technology (ICT) facilities and services check whether the items comply with the minimum standards defined in this policy and report any areas of non-compliance to ICTC.

PROCEDURES

A user issued with a password shall change it immediately after they:

- Have been issued with the initial default password.
- Have used the same password for more than six months.
- Are advised by NIS staff to change it.
- Have reason to suspect the password has been observed or compromised.

The Chief Information Officer may approve either exemption or part-compliance with this policy where the requirements of this policy cannot be fully implemented in a particular ICT facility or service for operational reasons. When exemptions or part-compliance with this policy are approved, the details of the approval will be forwarded to ICTC for noting.

Non-compliance

Any breach of this policy will be managed in accordance with the ICT Breach Management Policy.

Web Server Standards Policy

PURPOSE

The purpose of this policy is to minimise risks to the University that may arise as a result of incorrect information being made available through unauthorised Ndejje web sites, and to ensure that Faculties, Schools and other organisational units have access to reliable web facilities and infrastructure.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

The Chief Information Officer may approve exemption or partial compliance with this policy where technical or operational reasons preclude full adherence.

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

Material with Ndejje URLs shall only be published on an Authorised web server. Authorised Web servers shall be managed to present a professional image of the University. Authorised web servers shall conform to NIS standards for server equipment, configuration and management.

Any material published electronically at Ndejje that is found to be in breach of any Federal or State legislation, any Ndejje Policy, or that significantly restricts or impacts on resources available to others may be removed without notice by authority of the Chief Information Officer.

International, Commonwealth, State and Local laws and the rules and statutes of the University shall take precedence over any policies contained within this document.

PROCEDURES

Registration and Approval

Except where approval has been granted by the Chief Information Officer or delegate, no web server shall be accessible via the World Wide Web beyond the Ndejje communications network.

NIS shall maintain a register of Authorised web servers. Information contained in the register shall include web servers' physical and network addresses, and details of staff responsible for their maintenance. NIS may from time to time use information collected in the registration process to contact staff responsible for the maintenance of Authorised web servers.

Before material with a Ndejje URL may be made accessible beyond the Ndejje communications network, the web server on which the material is stored must be registered with NIS, and the configuration of the server must be compliant with the provisions of this policy. To request registration of a web server and thus enable it to publish material on the internet, the Web Server Registration form must be completed and provided to NIS.

Authorised web servers shall be managed to assure maximum availability for University clients. Down-time shall be scheduled with adherence to NIS change management procedures.

Web Server Management

Each Authorised web server must be managed by a designated officer who is part of a recognised ICT team to ensure appropriate levels of technical backup. The officer must be appropriately experienced to professionally manage the Authorised web server. Such officers must be authorised by their executive manager or delegate to act as the point of contact on matters related to the web server(s) in their charge.

The designated officer's name shall be registered with NIS as part of the web server registration process to ensure that contact may be made promptly as necessary.

Compliance

NIS shall from time to time survey Authorised web servers to determine:

- the hardware in use;
- the server operating system in use;
- the web server software in use;
- the latest systems patch installed;
- the latest server application patch installed.

Where any Authorised web server is found to be being managed in contravention of the provisions of this Policy and Procedures, steps may be taken to restrict access to it from beyond the Ndejje communication network after reasonable consultation with the member of staff responsible.

OTHER RELEVANT DOCUMENTS/LINKS

NIL

ICT Monitoring Policy

PURPOSE

To ensure that the monitoring and inspection of information stored on University Information and Communication Technology (ICT) facilities and services is done in an appropriate and responsible manner.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

Records created by University staff during the course of University business are owned by the University and as such form part of Ndejje's corporate assets.

Electronic information stored on University ICT facilities and services may be subject to disclosure.

The University monitors electronic information and may inspect it, including electronic messages, in the following situations:

- Where it is required by law;
- Where it believes that violations of law or violations of University policy have taken place;
- To enable internal investigations into alleged misconduct to take place;
- To enable operational management of ICT facilities and services; and,
- To satisfy the requirements of the Freedom of Information Act 1992.

A staff member inspecting electronic information on behalf of the University is bound by the requirements of the Staff Confidentiality Agreement.

PROCEDURES

Authorisation to inspect electronic information

Inspection of electronic information shall occur only once it has been authorised in writing by any of the following:

- The Vice Chancellor or delegate;
- The University Secretary or delegate;
- Director of ICT or delegate;
- The Chief Information Officer or delegate.

Where it is believed the circumstances may lead to investigation of potential breach of Ndejje policy, the requester shall also consult with the Director Staff Services or Director Student Services (as appropriate).

Non-compliance

Any breach of this policy will be managed in accordance with the ICT Breach Management Policy.

OTHER RELEVANT DOCUMENTS/LINKS

NIL

ICT Policy Definitions

The following definitions apply to all sections of the ICT Policy Manual:

Appropriate and responsible manner means use that is consistent with the teaching, learning, research, University-based consultancy, and administrative objectives of the University and with the University Ethics and Social Justice Commitment Statement; it includes incidental personal use of University facilities and services.

Appropriate use means use that is consistent with the teaching, learning, research, University-based consultancy, and administrative objectives of the University and with the University's Guiding Ethical Principles; it includes incidental personal use of University facilities and services.

Authorised web server means a web server that is registered with Ndejje IT Services and approved to publish material on the internet.

Breach means an information security incident that involves users not using Information and Communication Technology (ICT) facilities and services in an appropriate and responsible manner.

Business Owner means an authorised University officer or his/her delegate responsible for the management of a work area. A Business Owner authorises access to controlled ICT services.

Business or purpose of the University means an action or requirement which the University needs to have directly performed or met, in order to meet its objectives; or an action or requirement which will facilitate the achievement of the University's objectives.

NIS means Ndejje Information Technology Services.

Controlled ICT service means an ICT service that only allows a user access after successful use of a username and password to authenticate themselves.

Copyrighted content means material for which the copyright for the content is held by a third-party other than the University, eg music, computer software, films, video.

Ndejje communications network means that network of electronic communications equipment identified by Internet Protocol (IP) addresses within the ranges used by the University.

Ndejje URL means a particular set of information on the Internet at a location with a Uniform Resource Locator that refers to a host either within the "ndejjeuniversity.ac.ug" domain or within the IP address ranges used by Ndejje.

Electronic Messaging Services means information technologies used to create, send, forward, receive, store, or print electronic messages.

Electronic Identity means the set of essential information about an individual that is stored electronically by the University.

Electronic Identifier means the value that is used in Ndejje electronic systems to uniquely identify an individual. An electronic identifier is an attribute of the electronic identity.

Electronic Information means any information or recorded, either mechanically, magnetically, or electronically, within Ndejje ICT facilities and services, including data, messages, music, computer software, films, video, etc.

Executive Manager means senior staff who have managerial responsibility for organisational area(s) within the University.

ICT means Information & Communication Technology.

ICTC means Information and Communication Technology Strategy Planning Committee.

Information and Communication Technology (ICT) facilities and services means any information resources provided by the University to assist or support teaching, learning, research and administrative activities. This includes, but is not limited to, physical spaces designated for teaching, study or research,

all digital and electronic information storage, software and communication media devices, including, but not limited to, telephone, mobile phones, wireless or computer networks, computer workstation equipment including laptops, personal digital assistants, electronic email systems, internet, intranet and extranet. ICT facilities and services covers all types of ICT facilities owned or leased by the University, ICT services provided by the University and computer equipment owned or leased by users which are used to connect to the University networks and/or the Internet

Incidental personal use means infrequent and minor use of ICT facilities and services that does not: (a) interfere with University business operations; (b) breach any Federal legislation, State legislation or University policy; (c) breach an ICT vendor's conditions of use or licence agreement.

Information security incident means any information security event that disrupts the expected standard operation of ICT services and facilities.

Infrastructure means the physical equipment used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, and also the router, aggregator, repeater, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals and data that are transmitted.

Malware means software written for malicious purposes such as computer viruses, worms, Trojan horses and spyware programs.

Objectionable material as defined by the State as sexually explicit material (including that involving children), incitement to violence, torture, and bestiality.

Operating System(s) means the main control program that runs a computer and sets the standard for running application programs. It is the first program loaded when the computer is turned on, and it resides in memory at all times. An operating system is responsible for functions such as memory allocation, managing programs and errors, and directing input and output.

Personal web server means equipment that normally functions as an individual person's desktop workstation that has been configured to publish material at a web URL.

Pornography means sexually explicit material that is not Objectionable material.

Qualified means having formal certification for administration of a relevant web server and its related operating system or evidence of successful completion of training courses and/or self-paced modules pertaining to the web server software and related operating system being used in a particular School or Area, or equivalent experience.

Record means any record, irrespective of format, created or received by an individual or group working on behalf of the University that relates to a business activity of the University and is kept as evidence of such activity.

Restricted material as defined by State, includes any material that a reasonable adult, by reason of the nature of the material, or the nature or extent of references in the material to matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena, would regard as unsuitable for a minor to see, read or hear.

SEMS means Student Electronic Messaging Service.

Software means a specific use for a computer program, such as for accounts payable or payroll. The term is commonly used in place of the terms "application", "operating system" or "program." Examples of programs and software include pre-packaged productivity software (such as spreadsheets and word processors) and larger, customised packages designed for multiple users (such as e-mail).

Staff member means any person who has been offered and has accepted a contract of employment with Ndejje University.

Student means a person who is admitted to, or enrolled in, a unit, course or program of study approved by Ndejje University, which leads to, or is capable of leading to, an academic award of the University. For the purposes of this definition, the academic awards of the University are as recorded in the List of Academic Awards of Ndejje University.

Student Electronic Messaging Service or *Student E-mail* means the electronic messaging services provided by the University to students via the University student portal and intranet.

University Associate means a person affiliated with and/or providing services to the University.

URL means Uniform Resource Locator, and defines the global address or location of a particular set of information on the World Wide Web.

University means Ndejje University.

Use of Electronic Messaging Services means to create, send, forward, reply, copy, store, print, or possess electronic messages. For the purpose of this procedure, receipt of an electronic message is excluded from this definition to the extent that the recipient may not have control over the content of the message received.

User means a staff member, student or University Associate of Ndejje University, and includes other persons given limited access to University ICT facilities and services in support of the teaching, learning, research, University-based consultancy, and administrative objectives of the University.

Virus means a particular type of software written for malicious purposes; viruses are part of the “malware” family.

Web server means a computer that publishes electronic information via either the http or https protocols.

World Wide Web means a system of Internet servers that support specially formatted documents. The documents are formatted to support links to other documents, as well as graphics, audio, and video files.

RESPONSIBILITIES	
Policy Manager	Systems Manager
Contact	Systems Manager
Tel : 0772406005	
Email: nvirimoses@ndejjeuniversity.ac.ug	
Review Date	1 July 2011

REVISION HISTORY:

Revision Ref. No.	Approved/ Rescinded	Date	Committee/ Board	Resolution Number	Document Reference
New					
Amended					