UNIVERSITY OF UYO
UYO

....ICT Driving the World

INFORMATION AND COMMUNICATIONS TECHNOLOGY
(ICT) POLICY

DECEMBER, 2015

UNIVERSITY OF UYO
UYO

....ICT Driving the World

INFORMATION AND COMMUNICATIONS TECHNOLOGY
(ICT) POLICY

DECEMBER, 2015

FOREWORD

Information and Communications Technology (ICT) has become an enabling tool for any activity and business process of an organization. It is a technology that is used for the processing and distribution of data/information using computer hardware and software, telecommunications, and digital electronics.

ICT resources remain central to University functions, activities and roles. Its application and usage requires coordination from a central unit, and the Directorate of ICT has been saddled with this responsibility.

Consequent upon this, the University of Uyo has set out this ICT policy as an underlying guideline for proper monitoring and control towards ensuring efficient and effective use of ICT facilities to achieve its mission and vision. This ICT policy document therefore articulates policy guidelines and framework as programmes of action that will guide the University in the development and application of ICT facilities by all units of the University for the support of teaching and learning. This will be achieved by integrating ICT into teaching, learning, research, information dissemination and management of activities to close the knowledge and technology gap that hitherto exists within the system and place global information grid at the disposal of the University community.

Prof. Enefiok Effiong Essien
Vice Chancellor,
University of Uyo, Uyo

Table of Contents

DEFINITIONS AND ACRONYMS

Academic Data: Refers to data, which contain information on University academic profiles such as courses/curricula enrolment, degree/transcript, course/examination timetables and alumni.

ASUU: Academic Staff Union of Universities

Centralized Distributed System: A collection of independent computers that appears to its users as a single coherent system. A distributed system consists of a collection of autonomous computers, connected through a network and distribution middleware, which enables computers to coordinate their activities and to share the resources of the system, so that users perceive the system as a single, integrated computing facility

Council: The University of Uyo Governing Council

CRU: Computing Resources for Users

Data: The quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media. Data is distinct information that is formatted in a special way. Data exists in a variety of forms, like text on paper or bytes stored in electronic memory.

DCN: Data Communication Network

Department: A unit within the University of Uyo offering one or more programme

DICT: Directorate of Information and Communications Technology

DIPR: Directorate of Information and Public Relation

Faculty: A unit within the University of Uyo with more than one Departments

Financial Data: Refers to data, which contain information on University financial profiles such as revenue, expenditure, budget, assets and facilities.

HOD: Head of Department

Human Resource Data: Refers to data, which contain information on the human resource profile of the University such as establishment, staffing level, procedures and manuals, benefit schemes and beneficiaries.

ICT: Information and Communications Technology

ICT Systems: The internet, intranet, e-mail, telephone and voicemail systems used in the course of University of Uyo activities.

ICT-PMC: Information and Communications Technology-Policy Management Committee

Information: Refers to all records, documents and data whether computerized or not and all software whether developed by the University of Uyo or otherwise acquired, that is owned by the University or entrusted to it for any purpose or used in the course of or associated in any way with the University of Uyo's business activities.

Information Management: Information management (IM) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences. This sometimes involves those who have a stake in, or a right to that information.

Library Data: Refers to data, which contain information on University library profiles such as subscribed journals, available print collections available special collections.

NAAT: National Association of Academic Technologists

NASU: Non-Academic Staff Union

Network: Local Area Network within the University of Uyo, as well as access to the Intranet, Internet and other networks using University of Uyo's facility.

NOC: Network operations Center

OSS: Open Source Software

Personnel Data: Refers to information relating to staff characteristics (qualification, rank, pension accrued, compensations, salary and so on) and staff demographics (state of origin, age, sex, religion, marital status, department, and so on).

Research Data: Refers to all outputs of creative work undertaken on a systematic basis in order to increase the University knowledge base and information

SSANU: Senior Staff Association of Nigerian Universities

Student Data: Refers to information relating to student characteristics (course and hall residence registration, academic performance, financial status) and student demographics (state of origin, age, sex, religion).

UNIUYO: University of Uyo

User: A person accessing, developing, implementing and/or using University of Uyo ICT infrastructure. All users of services provided by, or for which access is facilitated by University of Uyo including students, staff, visitors, partners, third parties, contractors, suppliers and associates.

VC: Vice-Chancellor

University of Uyo - Vision Statement

To be a centre of academic excellence by utilizing the available human and technological resources for teaching, research, community service and sustainable development.

University of Uyo - Mission Statement

To diligently pursue scholarship and deploy its output for human capacity development and economic growth in the society, with active participation in Information and Communication Technology, sensitivity to Nigeria's rich cultural heritage and responsiveness to global environmental changes.

1.0 INTRODUCTION

Information and Communications Technology (ICT) development over the last few decades has led to the convergence of broadcasting, telecommunications, computing and contents. It has impacted the way business is conducted, facilitated learning and knowledge sharing, and generated global information flows, empowered citizens and communities, resulting in a global information society. It is widely acknowledged to be the engine of economic growth and directly linked to productivity. ICT resources remain central to University functions, activities and roles. Therefore, their control and monitoring has to be coordinated for the entire University. Against this background, the University of Uyo in its vision towards world class excellence has set out this ICT policy as an underlying guideline for proper, efficient and effective support and development of ICT functions within University of Uyo (UNIUYO), as a means of utilizing the available human and technological resources for teaching, learning, research, community service and sustainable development.

This policy document, therefore, is a necessary guide for developers, users and managers of information and ICT resources on appropriate standards, that conform to recognized International standards and industry best practice for adoption by UNIUYO for the acquisition, development, usage and management of ICT resources to ensure availability and proper use and utilization of ICT in the executing UNIUYO functions.

1.1 STRUCTURES FOR ICT POLICY GOVERNANCE, MANAGEMENT AND IMPLEMENTATION

The governance and management of resources, development process, innovation, research and implementation of ICT policies, strategies and services are provided in this section.

ICT resources remain central to University functions, activities and roles. Therefore, their control and monitoring has to be coordinated for the whole University. However, the recommended approach for adoption by UNIUYO is the coordinated decentralization technique. To that effect the Directorate of Information and Communications Technology (DICT) shall coordinate all technical aspects of ICT activities including, training, ICT installations, supervision and monitoring of ICT Projects in the University, however Department of Computer Science shall serve as the research unit of DICT.

1.1.1 Basic Principles

This policy is based on the following principles, which must be adhered to by all those responsible for the implementation of this policy and to whom this policy applies:

a. The ICT resources of UNIUYO are provided to support the teaching, research, community services and administrative activities and any other business of University of Uyo;

b. Access to UNIUYO's resources, data/information and to external networks are granted to authorized users on the basis that the use of the ICT resources shall be responsible, ethical and lawful at all times;

c. Authorized users are required to observe UNIUYO ICT Policy, and the Nigerian Cyber Crime Laws.

d. Data and information relating to persons and other confidential matters acquired for business purposes shall be protected.

e. University administrative and business information shall be protected from unauthorized and/or accidental disclosure.

f. UNIUYO ICT resources must not under any circumstances be used to humiliate, intimidate, or vilify others.

1.1.2 ICT Policy Management

The implementation and management of this policy shall be the responsibility of:

a. Information and Communications Technology-Policy and Management Committee (ICT-PMC)

b. The Directorate of Information and Communications Technology (DICT)

1.1.3 ICT-PMC

The ICT-PMC advises on the overall direction of ICT in the University, endorses the policy guidelines.

1.1.3.1 Composition and Terms of Reference of the ICT- PMC

This committee will be composed of people and ICT-users' stakeholders who are willing to contribute significant insights and to actively participate in high-level ICT policy formulation. The ICT-PMC shall be constituted by the Vice Chancellor (VC).

The terms of reference of ICT-PMC are:

a. to support in the development and enforcement of ICT standards, policies and procedures within Uniuyo.

b. to promote the harmonization of ICT developments and activities engaged by all units of the University.

c. to identify and promote areas of collaboration with other institutions to advance the use of ICT for teaching, learning and research

d. generate revenue for the University through a functional ICT provision and other ICT projects.

e. carry out any other functions assigned to it by the VC.

1.1.3.2 Members of the ICT-PMC shall be drawn from the following:

a. Administrator (to be appointed by the VC)

b. Director, DICT Chairman

c. Deputy Director, DICT

d. One Representative of the Registrar

e. Three representatives from DICT

f. Three representatives from Department of Computer Science (one of which shall be the HOD)

g. Three representatives from Department of Computer Engineering (one of which shall be the HOD)

h. One Representative from the Legal Unit

i. One Representative from the University Library

j. One Representative from Academic Staff Union of Universities (ASUU)

k. One Representative from Senior Staff Association of Nigerian Universities (SSANU)

l. One Representative from Non-Academic Staff Union (NASU)

m. One Representative from National Association of Academic Technologists (NAAT)

n. One Representative from Bursary Department

o. One Representative from the Directorate of Physical Planning

p. One Representative from Students' Union Government

q. One Representative from the Directorate of Internal Audit

r. One Representative from Faculty of Business Administration

1.1.3.3 The Directorate of Information and Communications Technology (DICT)

The DICT is responsible for the strategic leadership of the University's ICT, its advocacy, external positioning, policy, and implementation.

It shall also be responsible for:

a. the implementation of ICT policies, strategies and ensuring adherence to standards by the University.

b. providing ICT advisory services to the entire University Community.

c. providing strategic support for all University's ICT Infrastructure and Services with the help of its various functional units.

d. other assignments as may be given by the VC

1.1.3.3.1 Functional Units of DICT and their Responsibilities

The functional units of DICT and their responsibilities are as follows:

a. The Director/Deputy Director

i. The Director/Deputy Director of DICT shall be responsible for the ICT strategic planning, co-coordinating, supervising and management of quality assurance as well as management of information systems of the University.

ii. Shall Co-ordinate activities of the various units of DICT to ensure

that the ICT facilities and services are managed and delivered at the highest level of quality.

iii. Liaising with the DICT Units to prepare and maintain an up to date database on staff and students as well as basic statistics in the University.

b. Software Development Unit

i. Systems analysis and design

ii. implement and manage appropriate University information systems

c. Student Information Management Unit

i. management of Student Information

ii. provision of support services to students on University Portal utilization

d. Hardware Maintenance Unit

i. investigation, troubleshooting and provision of solutions to malfunctioning systems

Ii. system installation, maintenance and repairs

e. Data Centre Management Unit

i. provision of technical support

ii. management and security of the institution's data and Data Centre Infrastructure

f. Networking Unit

i. provision of strategic support for all University's ICT Infrastructure

ii. network infrastructure management and installation

iii. provision of Network Security.

g. Internet Administration Unit

i. ensure the availability of internet access across the University community at all times

ii. Internet control and management services

h Project Management Unit

i. design, implementation and management of appropriate University ICT projects

ii. monitor, review and evaluation projects

i. Training and Manpower Development Unit

i. promoting the use of e-learning tools and materials

ii. provision of training for staff and students on ICT skills

iii. provision of ICT consultancy services

J. User Support Unit (Helpdesk)

i. receive user requests and enquiries and communicate same to appropriate unit of DICT for resolution

Ii. provision of support services to users

iii. publish its dedicated telephone lines for users real-time human and automated-response support services.

2.0 SCOPE AND OBJECTIVES

This policy document aims at identifying those ICT services that can best support the University services; define a governance and management structure for the development and implementation of ICT policies, strategies and services; and define the role of the University's Directorate of Information and Communications Technology.

2.1 Scope

This document provides the policy framework for:

a. Promoting e-learning

b. Enhancing learning management system and library services

c. Development and use of management information systems

d. Managing ICT services and network infrastructure

e. Secured and acceptable use of ICT facilities

f. Use of internet services and applications

g. ICT procurements

h. ICT project management

2.2 Objectives

The objectives of this Policy are to:

a. provide guidance in the development, use and maintenance of a reliable, secure and cost effective ICT infrastructure that conform to recognize standards for the access of internal and external information and learning materials

b. provide guidelines and standards to guide users and decision makers in the development and use of ICT resources in the University.

c. ensure that ICT resources are used effectively and efficiently in support of teaching, learning, research and administrative functions of the University.

d. encourage and create awareness so as to enable users to understand their responsibilities in protecting ICT resources

e. ensure that ICT resources are secured and protected against abuse, damage, loss or theft.

f. prevent/protect the system from attack to ensure the confidentiality, integrity and availability of data/information and ICT resources within the University.

P O L I C I E S:

Policies are guidelines to actions.

3.0 ACCESS MANAGEMENT AND CONTROL

The University shall harness ICT potential to enhance the services it offers to its staff and students. The purpose of access management and control shall be to define required access control measures to all Uniuyo systems and applications to protect the privacy, security, and confidentiality of Uniuyo information assets and systems.

In this section the following shall be considered:

a. ICT Infrastructure

b. Third Party Access

c. Network Control

d. Operational Environment

3.1. ICT Infrastructure

ICT infrastructure consists of three major components:

a. The data communication network (DCN)

b. The network operations center (NOC)

c. The computing resources for users (CRU)

3.1.1 Data Communication Network (DCN)

Data communications network infrastructure provides the essential link between users of information and sources of information. It comprises:

a. a data backbone cable linking all buildings of the University campus

b. individual local area networks for all administrative and academic buildings at each University campus

c. wireless infrastructure, servers, switches, routers and radios.

i. The University shall manage and control ubiquitous and equitable

access to ICT resources for students and staff through the establishment of network infrastructure in all work areas of students and staff.

i. The university shall provide access to ICT services located within the University network and on the Internet.

ii. Such access shall at all times be governed by the University network acceptable use policy.

iii. Procedures shall be established to prevent anticipated threats that may damage physical ICT devices.

iv. Appropriate precautions shall be established to protect electrical devices from power surge and data loss that may occur as a result of electrical power interruption and fluctuations by installing appropriate power conditioning equipment (e.g. UPS, Surge Protector, Inverter, Stabilizer etc.)

v. All devices shall be installed by authorized ICT staff only.

3.1.2 Network Operations Center (NOC)

Network Operations Center (NOC) is the home for all backend servers and related equipment that provide the hardware platform for the central network services of the University.

i. the NOC shall be locked at all times.

ii. entry to NOC and interference with ICT network equipment is strictly prohibited.

iii. Access to NOC shall be restricted to designated members of staff of the DICT/ICT_PMC. Any other necessary access must have prior written consent of the Director of DICT.

iv. provisions shall be made for services peculiar to specific Departments/Units with acceptable rationale for central hosting.

3.1.3 Computing Resources for Users (CRU)

The computing resources for users (CRU) consist of ICT equipment (computers and related accessories) that the University community uses to access the various network services.

i. adequate access time shall be provided for users through the provision of sufficient computing facilities and access times.

ii. connection to the University network whether owned or leased by users shall only be enabled when appropriate and updated antivirus software is available.

iii. All authenticated computers, workstations and laptops, personal digital assistant (PDA) and smart phones or other removable storage devices such as universal serial bus (USB) drives or memory sticks and other such devices may be connected to University network.

iv. Both outdoor and indoor ICT equipment shall be adequately protected against fire, water and physical damage.

v. All ICT equipment shall be ergonomically correct and shall not entail physical or physiological impact or damage for users.

3.2 Third Party Access

These are entities outside the University that may have access to the University ICT infrastructure.

i. Entities other than the University may neither negotiate nor grant third party access to the University's ICT resources.

ii. The University shall ensure that whenever certain portion of its institutional data are generated and maintained by an external party, for example; University of Uyo examination results, transcripts and fees payment at respective banks, appropriate procedures and guidelines are developed to guide the exchange of such data.

iii. Clearance shall be sought from the VC for any third-party network connection.

3.3 Network Control

Network control involves providing adequate barriers and controls that secure the University's network infrastructure from intruders, hackers, virus, worms, e-mail spam and other disruptive software. Network control shall be achieved through the following:

a. Physical access control

b. Logical access control

c. Antivirus

3.3.1 Physical Access Control

Physical access control refers to appropriate barriers and controls governing the physical access to and the maintenance of the integrity of critical University ICT network assets.

i. Access to ICT installations shall be to only authorize persons.

ii. Sign posts shall be erected showing “Restricted Area” at entrances of secured network infrastructure.

iii. All units and offices shall label all ICT equipment appropriately for proper identification

iv. A logbook or electronic system shall be maintained at the server room to record entries and departures by ICT personnel, visitors and service providers. Details of date, time, personnel/student/staff, purpose, and exit time shall be recorded in the logbook.

v. All units and offices shall be required to maintain an Asset Register to record and track each piece (e.g. a computer, laptop, printer in an

office) or group (in a computer laboratory or server room) of equipment.

vi. A centralized Asset Register shall be maintained to track all ICT equipment in the University.

vii. No computer equipment and related accessories shall be carried out of the computer laboratories unless the Dean of the respective Faculty or Head of Department has given explicit permission. The faculties shall maintain an ICT Asset Register where such moves are monitored and tracked.

viii. During non-working hours, all ICT resources in different Department/Units/Directorates shall be secured and protected against physical intrusion by appropriate access control, locks and surveillance systems or by security staff.

ix. Provision (e.g., pigeon holes) shall be made for safe keeping of student bags in the computer laboratories; bags shall not be allowed into the computer laboratories.

x. All students and staff shall be required to identify themselves (either physically or electronically) for access to computer laboratories and or facilities.

xi. Restriction shall be placed on deliberate activities that may result in one of the following:

- Wasting of ICT support staff time in support of systems
- Corrupting or destroying other users data
- Violating the privacy of other users
- Denying services to other users

3.3.2 Logical Access Control

Logical access control refers to electronic access control whose purpose is to limit access to data files and computer programs.

i. User accounts (staff, students, management and guests) shall be created for the purpose of managing and controlling logical access to the network.

ii. The user accounts shall comprise of user IDs and passwords

iii. All users shall obtain their password at the ICT helpdesk

iv. All staff shall have a valid user account for official (where necessary) and authorized personal uses. Such account shall be disabled not later than three months after the staff member leaves the services of the University.

v. All registered students shall have a valid user account to enhance lawful use in the pursuit of their studies. Such account shall be disabled not later than three months (for Postgraduate) and one month (for Undergraduate) after the student leaves the University.

vi. All Principal Officers of the University, College, Faculties, Institutes, Departments and Units shall have management account for official uses. Such accounts shall be transferred to incoming officers at times of change in administration.

vii. All intending users who are in the University for official duties e.g., external examiners and visiting staff from other institutions shall have a guest account. Application for this category of accounts shall be through the Head of Department or Unit to which the visitor is affiliated. Such account shall be disabled immediately the visitor leaves the University.

3.3.3 Antivirus

These are software utilities that protect the computers and networks from electronic virus infection.

i. The University shall provide a secure computer working environment by providing protective antivirus software designed to detect, remove and defend all University computers against malicious software, malware or viruses.

ii. The University shall ensure that approved licensed antivirus software from known and trusted sources is installed on all ICT facilities owned or leased.

iii. A computer virus management guideline shall be implemented at appropriate points of the University's network.

iv. For computers not connected to the network, the officer in charge at the Departments/units shall liaise with the DICT to have updates run on their computers at regular intervals.

v. All software or data received from any external source, including the original manufacturer and the Internet shall be treated as suspect until it has been scanned for viruses using the University's approved licensed virus detection software.

vi. Any virus incident or activity noticed by users on University computers owned or leased shall be reported to the ICT helpdesk for immediate action and containment.

vii. The DICT shall immediately disconnect such compromised ICT facilities and services from the University's network and these will remain disconnected until the infection has been remedied.

3.4 Operational Environment

This refers to the environment within which the ICT equipment is operated. The working environment for all ICT facilities will have the following:

a. Power supply

b. Air conditioning

c. Lightings

d. Fire detectors and extinguishers

e. Cleaning tools

3.4.1 Power Supply

This consists of:

a. Standby generators
b. Battery banks or inverters especially for centralized systems.
c. Uninterruptible Power Supply (UPS)
d. Stabilizers
e. Power surge protectors

i. The University shall ensure that power supply to computers and accessories shall be clean, safe and uninterruptible.

3.4.2 Air Conditioning

Air conditioning systems provides cooling that keep the operational environment of the ICT facilities within the equipment manufacturers' recommended specifications for temperature and humidity all year round.

i. The University shall ensure that server rooms and computer laboratories are equipped with functional air conditioning systems that operate at all times.

3.4.3 Lighting

This is a device that provides illumination.

i. The University shall ensure that the server rooms and computer laboratories are provided with functional lighting that operates at all times.

3.4.4 Fire Detector and Extinguishers

These are devices used to detect and extinguish fire.

i. All computer laboratory and server rooms shall be equipped with smoke detectors and fire alarm systems.
ii. Fire extinguishers shall be provided for computer laboratories and server rooms. They shall be periodically tested to ensure that they are in good working condition.
iii. All IT personnel shall periodically be made to undergo fire prevention drills.

3.4.5 Cleaning Tools

These are tools used for keeping the operational environment clean and tidy.

i. The server room, computer laboratory and computers shall at all times be kept clean of dust, dirt and rubbish.
ii. Eating and drinking shall be prohibited at the computer laboratory and server rooms.
iii. The computers shall be kept clean and free from contamination.

4.0 ACQUISITION OF ICT EQUIPMENT, INFRASTRUCTURE AND SERVICES

ICT equipment purchase budget determines how much money and goods are needed to reach desired goals in ICT development in the University. It also provides a representation of what the DICT plans to buy for the inventory and how much inventory it plans to grow or hold over a given period of time.

i. The DICT shall make annual budget to cover equipment purchases, equipment maintenance, internet bandwidth, software licenses and communications.

ii. Recurrent funding shall be adjusted as the inventory of equipment changes.

iii. The budget shall be subject to the approval of the VC.

iv. The DICT shall ensure that the right equipment are procured, installed, maintained and repaired in good time. This policy shall guide the ICT Staff as well as those in the Departments/Units/Colleges/Faculties/Directorate.

v. All donated ICT equipment shall be subject to specification and standardization test and shall be rejected by the DICT where the equipment fails the conformity test.

vi. The procedures shall also ensure that the ICT equipment and services to be procured meet the following criteria:

- are of satisfactory quality and are compatible with the balance of the project;
- shall be delivered or completed in timely fashion; and,
- are priced so as not to adversely affect the economic and financial viability of the project.

vii. Various departments shall also follow the correct procedure for

procurement of ICT related goods and services.

viii. The DICT shall be responsible for acquisition of all ICT equipment based on approved specification.

ix. All requests for ICT equipment shall be routed to the Vice Chancellor through the Director of ICT.

x. The DICT shall assist the Departments with preparation of technical specifications whenever the need arises.

xi. All donated ICT equipment to Departments, Faculties, Colleges or Units shall be routed through the DICT.

xii. All donated ICT equipment shall be forwarded to the benefiting departments, faculties, colleges or units subject to availability of space.

xiii. In the case of Computer systems, individuals/departments shall be given full privilege to administer the system and shall be responsible for the provision of adequate operating environment (floor space, climate control, ventilation, etc.) for the system.

5.0 REPAIRS, DISPOSAL AND DISASTER RECOVERY

Maintenance of ICT infrastructure is very crucial in the provision of a central and sustainable ICT services in the University. This is achieved through a co-ordinate activity that involves repairs and appropriate disposal of infrastructure as well as adequate disaster recovery mechanism.

In this section, the following shall be considered:

a. Troubleshooting, Repairs and Maintenance

b. Disposal of Computers

c. Disaster Recovery and Contingency Plan

5.1 Troubleshooting, Repairs and Maintenance

It is the responsibility of the DICT to provide a centralized technical support on all aspects of ICT including hardware and software.

i. All faults on ICT devices in all units of the University must be reported to the Directorate of ICT for repairs and maintenance

ii. All repairs of Computers, Printers and other computing devices shall be handled by the Hardware Maintenance Unit of the DICT.

iii. The DICT shall carry out yearly audit of ICT equipment to ascertain performance, which shall form the basis for replacement plan, and report submitted to the DICT for appropriate action.

iv. No third party shall be allowed to work on any ICT equipment owned/managed by the Institution without permission from the DICT.

5.2 Disposal of ICT Equipment

Before disposing of any computer system, part of or any other ICT equipment, all the information/data stored on the system must be safely destroyed. The following policies shall be applied when disposing of such equipment:

i. Disposal of devices shall not endanger the environment or constitute its abuse and shall follow disposal instructions in the manual of the respective Hardware.

ii. All computers should be fully formatted and restored to factory default before they are disposed of.

iii. All expired ICT equipment or equipment whose faults can no longer be fixed shall be returned to the Hardware Maintenance Unit for proper disposal subject to approval by the DICT.

iv. Any ICT equipment that is not serving the required purpose shall be returned to the DICT on the recommendation of the Hardware Maintenance Unit.

v. All replaced ICT equipment shall be returned to Hardware Maintenance Unit.

5.3 Disaster Recovery and Contingency Plan

Disaster recovery and contingency plan specify the guidelines, resources, actions and personnel that are required to reinstate/restore the University information/database in the event of any loss that may arise from fire, vandalism, natural disaster or system failure. Contingency planning also ensures that internet, data and other mission critical systems do not go down for a time beyond 24 hours.

i. Adequate backup systems and contingency plans shall be maintained and regularly tested for disaster recovery readiness.

ii. All Units of the University must maintain regular backups of their data.

iii. The DICT shall make Data backup guideline and make it available to all units of the University.

iv. ICT related hardware contract should not be approved without expert advice and recommendations of the DICT.

6.0. ICT INFRASTRUCTURE DEVELOPMENT

ICT Infrastructure offers a range of technologies to assist an organization in running effectively.

In this section, the following shall be considered:

a. ICT Routes and Cabling

b. New and Existing Buildings

c. ICT Project Management

6.1 ICT Routes and Cabling

i. Planning of ICT routes and cabling shall be in conformity with Academic plan proposal, Master plan layout and proposed location for future development.

ii. ICT services that entail routing of cables along the University grounds shall be cleared with the Directorate of Physical Planning and the Department of Works for minimal disruption to existing underground service lines.

iii. All ICT cable lines outside buildings shall have concrete marker posts to define its route for ease of identification.

iv. Installation of ICT cable lines shall follow best practices in the profession to minimize damage to underground cables.

6.2 New and Existing Buildings

i. Effective earthing and lightning protection shall be provided for all new and existing buildings with ICT installations.

ii. The DICT shall ensure that the earthing and lightning protections of buildings are regularly tested.

iii. Provision shall be made for data, voice and video points in all the buildings and other ICT requirement as requested by the DICT.

6.3 ICT Project Management

The University is committed to continuously improve the delivery of ICT solutions within approved budget.

i. The DICT shall prepare a rolling 5-year network development plan, advising the University Management on appropriate developments aimed at ensuring the adequacy of the University's ICT infrastructure. This plan will take account of the University's strategic plan; usage and demand patterns; technological change; security; management and cost implications.

ii. The responsibility for the implementation of ICT Projects shall rest with the University Management and the DICT.

iii. The procedures shall conform to the University's rules, regulations and obligations and ensure that ICT projects for various departments are pursued diligently and effectively.

iv. The establishment and management of ICT Centers rest with the DICT, the University management and beneficiary department/unit/faculties.

v. The DICT shall manage all ICT projects by planning, delegating, monitoring, evaluating and controlling all aspect of ICT projects.

vi. All ICT Projects shall have a properly constituted Project Implementation Team (PIT) which shall be constituted by the VC and membership shall include: Director of the DICT, Dean/Head/Director of the direct beneficiary faculty/department/directorate of the project.

vii. All ICT project staff members shall work together, share knowledge and information, and cooperate to deliver quality projects.

viii. The Project Sponsor has overall responsibility for ensuring that a

project meets its objectives and delivers the projected benefits and must ensure that the project maintains its business focus, that it has clear authority and that the work, including risks, is actively managed.

ix. For all ICT projects, detailed functional and technical specifications must be documented and signed off by the Project Sponsor and the Director of DICT.

x. All internal staffing requirements (both business area and IT Services) must be identified and included in the cost budget.

xi. All ICT projects shall be formally handed over to the DICT after ensuring that adequate training and documentation have been provided.

7.0 SOFTWARE ACQUISITION, DEVELOPMENT AND USAGE

The University's ICT infrastructure cannot be run without adequate attention paid to software acquisition, development and usage. Most of the Information Management processes involving staff and students are handled by various software.

In this section, the following shall be considered:

a. Pirated or Unlicensed Software
b. Software Development
c. Open Source Software
d. Operating System software
e. Software Uninstallation
f. Software Copying
g. Software Storage
h. Software Review and Updates

7.1 Pirated or Unlicensed Software:

Software piracy is the mislicencing, unauthorized reproduction and illegal distribution of software, whether for business or personal use.

i. No pirated or unlicensed software shall be allowed on the University's computer systems.

7.2 Software Development:

Software development entails computer programming, documenting, testing, and debugging involved in the process of creating and maintaining applications and frameworks involved in a software development life cycle and resulting in a software product.

i. The University shall encourage the development of software by setting up well equipped Software Engineering Laboratory which shall be managed by the Software Development Unit of the DICT.

ii. All customized, developed and contracted software to be acquired by the University shall be tested, approved and recommended for use by DICT.

iii. The delivery, installation and maintenance of all acquired software shall be monitored by DICT.

iv. All software acquisition shall be done in conjunction with the DICT.

v. Priority shall be given to in-house developed software.

7.3 Open Source Software

Open source software refers to software that can be freely used, changed, and shared (in modified or unmodified form) by anyone very often developed in a public, collaborative manner.

i. The DICT shall recommend to the University suitable Open Source Software for use to reduce the cost of licensing.

7.4 Operating System Software

i. The recommended operating system software for computers in the University shall be:

- Windows Operating System
- Macintosh Operating System
- Linux Operating System

ii. The University shall acquire the licenses to upgrade existing operating system software where necessary.

7.5 Software Uninstallation

i. Uninstallation of software shall only take place when it is formally agreed by the DICT and the concerned Unit/Department that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time or if removal can be reverse to status quo.

7.6 Copying of Software

i. Staff, Students and Guests to the University are prohibited from allowing outsiders or themselves making copies of software or soft documents other than those provided for in the relevant licensing agreements.

7.7 Software Storage

i. The DICT shall be responsible for storing the evidence of software acquisition documents, which includes; the original CDs, Receipts, Certificate of Authenticity and Users Manual.

7.8 Software Review and Updates

i. The upward review of software in use shall be carried out by the DICT annually.

8.0 FUNDING OF ICT EQUIPMENT AND INFRASTRUCTURE

ICT projects are fund-driven. The design, establishment and management of ICT projects require a lot of funding and financial processes. These finances are sourced, both internally and externally.

In this section, the following shall be considered:

a. Source of funding for ICT equipment and infrastructure
b. Management of ICT projects funding account

8.1 Source of Funding for ICT Equipment and Infrastructure

The provision of standard ICT services in the University requires a huge investment of funds. Possible sources of funds are:

a. University Budget through internally generated revenue or government capital project.
b. Public Private Partnership (PPP) joint venture between private company and public investment.
c. ICT Charges and fees from end-users - Students, Staff and the Public.
d. Training and support service by the DICT e.g. workshops and seminars.
e. Endowment placement or chair by individuals and corporate bodies.
f. Grants
g. Donation by Government and private Agencies e.g. Trust Funds, Education Tax Funds.
h. Surcharges and penalties.
i. Disposal of unserviceable items.
j. Other sources as may be approved by the VC.
    i. The University shall create a separate ICT budget annuall for ICT funding.

ii. The ICT budget votes shall have specific provisions for:

- Hardware acquisition
- Software acquisition
- Software license fee
- Hardware maintenance
- System development
- ICT technical staff training
- ICT user training
- ICT staff salaries
- Equipment spares
- Communication fees (Bandwidth servicing)

8.2 Management of ICT Project Fund Account

i. There shall be an ICT Projects Account opened in any bank approved by the Vice Chancellor.

ii. Authorized Signatories to the account shall be the VC or Deputy Vice Chancellor as “A” Signatories, the Director or Deputy Director of ICT as '”B” Signatories and Bursar or Deputy Bursar as “C” Signatories.

iii. All ICT Charges and fees from end-users - Students, Staff and the Public shall be deposited into the ICT Projects account.

iv. All moneys meant for ICT Projects shall be deposited into the ICT Project accounts.

9.0 DATA AND INFORMATION MANAGEMENT

Data and Information Management in any organization is very important and must be handled efficiently and professionally to avoid mismanagement and loss.

All Institutional data and information which includes; research data, library data, academic data, student data, human resource data, personnel data and financial data created, collected, maintained and recorded, shall be properly managed by the University and/or agents working on its behalf.

In this section, policies on the following shall be considered:

a. Data Storage
b. Data Confidentiality
c. Data Ownership
d. Copyright infringement

9.1 Data Storage

I. The University shall adopt a Centralized-Distributed database system of storage where each Unit/Department has its local database and a backup at the Central Storage to be managed by the DICT.

ii. The DICT shall ensure that each Unit/Department shall work out their own Data Security details.

9.2 Data Confidentiality

i. Authorized Users shall keep confidential all University data and Information provided in confidence to the University by other entities.

ii. Each staff member is under the obligation not to disclose University data and information unless authorized to do so.

iii. Data and Information shall be disseminated on a need-to-know basis and shall not be divulged to unauthorized persons

iv. Breach of confidentiality through accidental or negligent disclosure shall result in disciplinary action taken against the user.

9.3 Data Ownership

i. All information acquired or created by user while carrying out the University's business, except that which is specifically exempted as private or personal, shall be owned by the University.

ii. Each User Department shall have individual ownership of its own data resource and ensure that the data is accurate and backed up regularly.

9.4 Copyright Infringement

i. Copying, recording or processing information which infringes any patent or breaches any copyright is not allowed.

ii. Products created from work done for the University using the University's ICT resources shall be the property of the University and under no circumstances shall they be distributed or sold without proper authorization.

10.0 PROHIBITED USE OF UNIVERSITY'S ICT RESOURCES

Prohibited actions apply to the following list of activities when using the University's ICT resource:

a. Advertisements
b. Peer-to-Peer File Sharing (P2P)
c. Business activities
d. Unauthorized access
e. Pornography
f. Gambling
g. Computer Games

10.1 Advertising and Sponsorship

i. Paid advertisements shall not be permitted on any website using the University domain name except with the written permission of the VC.

10.2 Peer-to-Peer File Sharing (P2P)

i. Installation or use of peer- to- peer file sharing software shall not be is not permitted on the University's network
ii. Peer-to-peer file sharing for teaching and research activities shall be allowed but must be approved by the DICT, and only where no alternative technology is appropriate.

10.3 Business Activities

i. Users are not permitted to run a business or publish a journal/magazine using the University's ICT Resources except with the written permission of the VC.

10.4 Unauthorized Access

i. Users are forbidden from gaining unauthorized access or attempting to

gain unauthorized access to ICT Resources belonging to the University and other organizations from the via the University network.

10.5 Pornography

i. Users are not permitted to utilize the University's ICT Resources to access pornographic material or to create, store or distribute pornographic material of any type.

10.6 Gambling

i. Users are not permitted to utilize the University's ICT Resources to gamble.

10.7 Computer Games

i. Users are not permitted to utilize the University's ICT Resources to play computer games during office hours.

11.0 INTERNET, EMAIL SERVICES AND UNIVERSITY WEBSITE

The Internet facility is primarily provided to enhance learning, teaching, research and administrative functions of the University. The Internet complements the University's library for research materials and information dissemination.

In this section, the following shall be considered:

a. Internet Access Acceptable use
b. Data downloads
c. Electronic Mail (E-mail) Services
d. UNIUYO Website
e. Disclaimer

11.1 Internet Access Acceptable use

Large bandwidth without proper management will result in bandwidth wastage and a slow and inefficient system.

i. The University shall provide adequate bandwidth to meet the needs and demands of the users through the DICT.
ii. Only registered users shall be granted access information (username and password) to the Internet.
iii. Users must have an account to use the internet and the University e-mail services
iv. The same user cannot use the same password on two different computers within an hour interval.
v. Two people cannot use the same account at the same time.
vi. All logins shall undergo both processes of authentication and authorization.
vii. Passwords must not be given out or shared.
viii. User access and activity on the University network shall be monitored and logged
ix. Access to heavily used sites (e.g. Yahoo mail, Google, hotmail,

Facebook) is restricted between certain periods of the day whenever there is a need to do so. Users will be given adequate notice before such restrictions.

x. Appropriate filtering facilities for web based and non web based Internet traffic shall be provided to filter prohibitive and obscene websites with contents that do not have direct educational value e.g. pornography, gaming, advertorials, campaign links, sites with offensive materials relating to ethnicity, religion and gender.

xi. The University shall restrict or suspend access to any user and at any time whenever this policy is breached.

11.2 Data Downloads

i. The size of data that can be downloaded is limited at specific times of the day

ii. Unauthorized downloads, installation of programs or utilities that may flood the network, causing denial of service to other users shall be restricted.

iii. Downloading of multimedia-based files will be restricted, unless permitted by the DICT.

iv. Any computer/user causing excessive traffic congestion shall be automatically blocked after some time.

v. The University's internet facility shall not be used to propagate any malicious software (virus) or software that disrupts or damage computer systems.

11.3 Electronic Mail (E-mail) Services

E-mail services provide users with the means to exchange digital messages using a store and forward mechanism. E-mail systems accept, forward, deliver and store messages on behalf of users who only need to connect to the e-mail infrastructure for the duration of message submission to, or retrieval from their designated server.

The e-mail facility has been provided by the University to enhance faster communication and interaction among the staff and students.

The following shall be considered for the University's e-mail services:

a. UNIUYO e-mail account
b. Closure of UNIUYO e-mail account
c. Mailing lists

11.3.1 University E-mail Account

UNIUYO e-mail service is available for all staff and students under the official University domain name (uniuyo.edu.ng) governed by the University's mail policy. The e-mail account is divided into two groups:

a. Personal e-mail account: for the personal and professional use of the staff or students (tied to the name of the user).
b. Official e-mail account: strictly for official correspondence (tied to an office/post).

i. Users shall be required to have a UNIUYO e-mail account which will be issued after approval by the authorized officer.
ii. The e-mail addresses (personal and official) shall have a standard format which all users conform with.
iii. Only staff and student shall hold a University e-mail account
iv. E-mail shall be an acceptable means of disseminating official information (memos, notices) to the University community.
v. Official internal information (as in iii) disseminated through e-mail shall be through UNIUYO's e-mail account.

vi. All official correspondences and public interaction shall be via the UNIUYO's e-mail account.

vii. Staff shall be expected to check and reply to official e-mail message within 24-hours (working days).

viii. Students shall be expected to check and reply to all official e-mail messages with 48-hours (working days).

ix. Users are NOT allowed to:

· Use of UNIUYO's e-mail account for spamming

· Use unethical languages in e-mails.

· Falsely represent the University, assert or imply that personal views or opinions are the institutional view or opinion of the University.

· Use the e-mail account for any commercial purpose.

· Send mass e-mail to a wide sub-set of users in the University without appropriate privilege or permission.

· Use the e-mail account for disseminating offensive materials relating to ethnicity, religion or gender

· Use the e-mail account for propagating negative impressions against the University management

x. Users shall be expected to ensure:

- Their access information (username and password) are kept private and promptly report in case compromise is suspected. Users are held accountable for any e-mail sent using their account.
- Confidentiality and privacy of official information is upheld: official information is not circulated beyond the bound of the UNIUYO e-mail domain.
- Attachments sent are virus-free.

11.3.2 Closure of UNIUYO E-mail Account

i. The UNIUYO e-mail account shall be closed or disabled as soon as practicable for staff in the following category:
   - Dismissal: The e-mail account shall be closed immediately
   - Resignation: The e-mail account shall be closed within 6 months.
   - Retirement: The e-mail account shall be closed based on approval.
   - Death: The e-mail account shall be closed immediately.

ii. The UNIUYO e-mail account shall be closed or disable for students in the following category:
   - Rustication: The e-mail account shall be closed immediately
   - Graduation: The e-mail accounts of graduating students shall be closed one month after graduation.
   - Death: The e-mail account shall be closed immediately

11.3.3 Mailing Lists

i. Mailing lists shall be created to facilitate communications and dissemination of information in the University

ii. The University Staff Mailing List shall be used to disseminate information to and among staff.

iii. Postings to the University Staff Mailing List shall be restricted to messages from the VC, Registrar, statutory boards, committees and others as approved by the VC or Registrar

11.4 UNIUYO Website

It is the policy of the University to have an official website (uniuyo.edu.ng) that showcases the University to the rest of the world in disseminating current and up-to-date information from all organs of the University (Faculties, Colleges, Departments, Directorates, Centres, Institutes and Units). The purpose of this website is to provide the staff and students of University with the necessary information

about the functionality of the University website as an effective communication medium for the benefit of the University community and the world at large. The website will amongst other things:

a. Enhance the University's presence on the internet and broaden recognition for the University, while strengthening its image.
b. Enhance the quality of the UNIUYO website through the publishing of current and informative content in an acceptable web manner.
c. Support a sustainable information and communication infrastructure that supports the University's mission, goals and objectives through an on-line presence.
d. Optimize resources to streamline, and automate the development and maintenance of the UNIUYO website as a quick and easily accessible means of communication with the University's target audience.

i. UNIUYO web pages are the primary entrance points to the University's website and the appearance and content shall be the responsibility of the DIPR and the DICT.
ii. The DIPR and DICT shall always review the web pages to ensure that they reflect the same high level of quality and consistency as the University's print publication.
iii. The DIPR and DICT shall ensure that the content of the site conform to the mission and mandate of the University.
iv. Each Unit/Department/Directorate/College shall setup a committee to provide information to the Directorate of ICT for update of their web pages.
v. No Unit/Department/Directorate/Colleges shall be allowed to host

its website or web-pages outside the University's web server. Where this is deemed necessary permission shall be sought from the VC.

11.5 Disclaimer

i. The University shall not be responsible for materials viewed, downloaded or scammed by users from the internet.

12.0 E-LEARNING AND DIGITAL RESOURCES

Any technologically mediated learning using computers whether from a distance or in face-to-face classroom setting as in computer assisted learning.

In this section, policies on the following shall be considered:

a. E-learning Resources
b. Digital Resources
c. Digital Preservative/Archiving
d. Education, Research Development and Copyright
e. University Library
f. Capacity Building/ End-User Skills Development

12.1 E-learning Resources

i. The University shall leverage faculty/unit effectiveness by using ICT in instruction, learning and research.
ii. The University shall promote the integration of e-learning to improve the effectiveness of teaching, research and learning.
iii. The University shall promote the development of e-content to address the educational needs of the University
iv. The DICT shall develop University wide and global e-learning networks based on academic interests groups and research collaborations.
v. The University shall ensure continuous training and promotion of in-house e-learning training capabilities for all students and staff on a continuous basis to equip them with the requisite skills to fully exploit the e-learning tools in the various disciplines.
vi. The University shall collaborate and form global e-learning networks with other academic and research interest groups to facilitate sharing

of e-learning resources.

vii. Establish the appropriate common e-learning platform responsive to academic needs.

viii. The University shall provide greater access to University education through the development of ICT-based distance learning.

12.2 Digital Resources

Digital resources contribute to the commitment of the University to support research activities and are intended primarily as a repository for previously-published work, and not as an independent publishing platform for new research articles.

i. Researchers, authors, departments/units shall submit works for which they are the sole rights holders, or for which they have obtained permission to submit from all co-authors to the library.

ii. Works that may be submitted shall include; Theses and Dissertations, Journal articles, Working papers, Conference papers, Inaugural lectures and published books. The work will receive increased visibility while raising the profile of the University.

iii. All graduate Theses/Dissertations, Research Publications, Inaugural Lectures, Conference Proceedings etc, approved by the appropriate Board shall be submitted to the Library in soft copies.

iv. Minutes of all meetings and reports of statutory boards, committees and others shall be deposited at the office of the Registrar.

v. All relevant hard copies of documents e.g. Minutes, CVs etc, shall be digitized and archived at the designated ICT centers.

12.3 Digital Preservation/Archiving

The rapid growth in the number of digital resources and the University's budget used to obtain them has necessitated that proactive steps be taken to preserve these materials.

i. Digital preservation activities shall ensure that Departments/Units, Faculties, Staff, Students, and other users have ongoing access to the UNIUYO Library's expanding digital collections.

ii. UNIUYO Library shall be committed to providing access to digital materials while respecting and upholding the intellectual property rights of authors and obtaining prior consent when the creator's identity is known.

iii. UNIUYO Library shall observe current standards and best practices related to the creation, maintenance, storage, and delivery of digital objects and metadata, as determined by international, national, consortia, and local institutions and governing bodies.

iv. UNIUYO Library shall commit to on-going training and development of staff in areas related to digital preservation, as well as outreach to inform units/departments, faculties, students, and staff of the best practices for creating and maintaining digital objects.

v. UNIUYO Library shall fulfill the digital preservation objectives by developing and maintaining the necessary hardware, software, expertise, and protocols to ensure long term access.

vi. The specific preservation actions used for UNIUYO Library's digital resources shall rest heavily on the source and type of content, as well as the existing technology, expertise, and ongoing support.

vii. Digital objects shall be managed using the life-cycle model, which is a framework describing the stages that digital resources go through during their existence.

viii. All digital resources created by the UNIUYO Library shall adhere to the Library's pending Metadata policy.

ix. Digital resources shall be stored in a manner that is consistent with accepted best practices in the digital preservation community. This will include both technical infrastructure (hardware, software, network access, data backup, facilities, maintenance, etc.) and ongoing preservation management activities.

x. Best practices in digital preservation requires duplicating digital objects in both local systems and geographically removed systems and shall in due course pursue this by working with the DICT to host redundant/remote local storage.

xi. This policy and the actions that flow from it shall be evaluated regularly to ensure that implemented strategies continue to support the Library's mission and policies to provide up-to-date resources, use resources in a cost-effective manner, and adapt appropriately to address evolving technologies. This evaluation shall be completed at least once every 3 years.

12.4 Education, Research Development and Copyright

Education, research and development constitute the major arm of any University system where inventions, copyrightable works and other creative products of scholarship that have the potential to benefit the public through practical application may result from the activities of University employees in the course of their employment or through the

use, by University students or by any person, of University resources such as facilities, equipment, or funds.

i. Those participating in scientific or scholarly research shall maintain careful research records, to establish and follow well-defined protocols consistent with all State, Federal, and University guidelines, and to report discoveries, observations, and scholarly and artistic activities accurately and fairly.

ii. The University owns all rights, title, and interest in Tangible Research Property and Research Data developed with support from University Resources.

iii. The University shall own all rights, title and interest in Trademarks that relate to University Intellectual Property or relate to a program of education, service, public relations, research or training by the University.

iv. An author of an Instructional or Scholarly Copyrightable Work that is not University-owned shall be free to publish it, register the copyright in the author's name, and retain any revenues which may result therefrom.

v. The University shall require a written agreement from independent contractors that ownership of Copyrightable Works made in the course of a University retention will be assigned to the University.

vi. Each Instructional or Scholarly Copyrightable Work shall, by operation of this policy, be subject to a perpetual nonexclusive, royalty-free license from the author to the University to use, duplicate, and internally distribute the Instructional or Scholarly Copyrightable Work for any pedagogical, research, or educational purpose of the University, subject to attribution of original authorship

and to internal academic procedures and requirements of the department and school of origin of the Instructional or Scholarly Copyrightable Work.

vii. Inventors shall promptly in writing disclose and assign each Invention to the University and/or its designee, and shall not disclose any Invention to any third-party except as specifically authorized by the University or its designee.

viii. The University Intellectual Property Office shall facilitate institutional practices that support the University's research, education and development. This Office shall provide guidance regarding fair use and other copyright compliance issues and will advise the Vice Chancellor on issues regarding the application of copyright law by University staff, and implement a systematic, ongoing programme of copyright education and awareness suited to the rapidly changing technological and legal environments of higher education.

ix. University staff who desire to use copyrighted materials are responsible for ensuring compliance with the applicable copyright law, including making an initial good faith determination as to whether or not the desired use falls within the fair use exemption.

x. In the event of genuine doubt regarding the application of copyright law, the University staff should consult with the appropriate Office regarding such matters.

xi. The University shall preserve valuable and intellectual materials by converting them into digital forms.

12.5 University Library

i. In terms of ICT services, UNIUYO Library, supervised by the DICT will be responsible for creating and making available electronic-based library information resources for the purpose of teaching, learning and research. These include e-books, Online Public Access Catalogue (OPAC), digital repository, e-journals, information literacy, audio-visual services and CD-ROMs.

ii. The University shall improve both the efficiency and effectiveness of library operations and services through the implementation of an Integrated Library System (ILS). The ILS will be accessible within and outside the University's network.

iii. The University will support the integration of its library information resources with other interested academic and research groups to share and gain access to more information resources.

iv. The University shall continue to improve the infrastructure that will ensure easy access to the ILS.

12.6 Capacity Building/ End-User Skills Development

i. The University shall ensure and require that all students and staff are trained on a continuous basis to equip them with the requisite skills to fully exploit the ICT resources to enhance the discharge of their functions.

ii. The DICT shall recommend ICT trainings relevant for every section and forward requirements to the VC for financing.

iii. Staff of the DICT shall be trained on emerging technologies as the University may determine from time to time.

13.0 ENFORCEMENTS

Abuse of ICT privileges is subject to disciplinary action, which may include the loss of these privileges and other disciplinary actions.

i. The DICT shall for the purpose of enforcing this policy, document and audit user compliance from time to time.

ii. The DICT shall monitor and respond to network breaches as they occur

iii. The DICT shall temporarily suspend network access if an incident is determined to be interfering with the operations of the University network.

iv. The DICT shall determine the impact of any alleged violation of this policy and take, without notice, any necessary action if University resources and services are adversely affected to prevent immediate and further damage to the University network. Such actions may include:

- Suspension of an account
- Disconnection of systems or disable network ports
- Termination of running processes and programs
- Any other actions deemed necessary to restore network services.

v. Users shall be responsible for any financial loss to the University that results from inappropriate use of ICT resources.

vi. In the event that a user password is compromised, the DICT shall immediately reset the user's password to a one-time only password. Such actions are necessary to mitigate the risks from unauthorized access to University systems.

14.0 AMENDMENTS AND REVIEW

The ICT policy shall be amended annually and reviewed in five years. Members of the University community that wish to propose amendments shall write to the ICT-PMC.

15.0 CONCLUSION

Institutions of higher learning are today critically dependent on the smooth functioning of ICT and its services. A smooth functioning and running ICT can be assured only if establishment, operation and extension of ICT and ICT enabled functions are effected within a framework that takes full cognizance of the institutions overall strategic goals. As technology changes, planning becomes increasingly important in order to avoid incompatibility and inaccessibility. This ICT policy is a guide to actions to be pursued by the University as advantageous or expedient in its bid to optimize ICT development, usage and application in the University. It entails the vision, mission, goal, principles and plans that will guide the activities of all stakeholders.