FRAMEWORK AND GUIDELINES FOR ICT ADOPTION IN TERTIARY INSTITUTIONS".

National Information Technology Development Agency (NITDA)

August 2018
TABLE OF CONTENTS

1.0 INTRODUCTION ........................................ 1
  1.1 Background ........................................... 1
2.0 POLICIES ............................................ 2
3.0 SOFTWARE ACQUISITION, DEVELOPMENT AND USAGE .... 3
  3.1 Software Development ................................ 4
  3.2 Open Source Software ................................ 4
  3.3 Pirated or (Illegally Acquired) Software ............... 4
  3.4 Operating System Software .......................... 5
  3.5 Software Uninstallation ................................ 5
  3.6 Copying of Software .................................. 5
  3.7 Software Storage and Records Keeping ................. 5
  3.8 Software Updates and Upgrades ....................... 5
4.0 ACQUISITION OF ICT EQUIPMENT, INFRASTRUCTURE AND SERVICES .... 6
5.0 MAINTENANCE, DISPOSAL AND DISASTER RECOVERY ...... 6
  5.1 First Level and Routine Maintenance ................. 7
  5.2 Disposal of ICT Equipment, Devices and Software .......... 7
  5.3 Disaster Recovery and Contingency Plan ............... 7
6.0. ICT NETWORKING INFRASTRUCTURE DEVELOPMENT ........ 8
  6.1 ICT Backbone Infrastructure .......................... 8
  6.2 Backbone Network ..................................... 8
  6.3 ICT Project Management ................................ 8
7.0 ACCESS MANAGEMENT AND CONTROL ........................ 9
  7.1 ICT Infrastructure ................................... 9
    7.1.1 Data Communication Network (DCN) ............... 9
    7.1.2 Network Operations Centre (NOC) ................. 10
    7.1.3 ICT Services and Computing Resources for Users .... 10
  7.2 Network Control and Cyber Security .................... 11
    7.2.1 Assignment of Roles of Responsibilities ........... 11
    7.2.2 Unacceptable Use of Resources .................... 12
    7.2.3 Antivirus ........................................ 12
  7.3 Operational Environment ................................ 13
    7.3.1 Uninterrupted Power Supply ....................... 13
    7.3.2 Adequate and Well-Maintained Air Conditioning System 13
    7.3.3 Illumination ...................................... 13
    7.3.4 Fire Protection - Detector and Extinguishers ....... 13
    7.3.5 Cleaning Tools .................................... 14

ii
1.0 INTRODUCTION

1.1 Background

Information and Communication Technology (ICT) has become firmly established as a necessary tool for the smooth running of any university's Information Management strategy and associated core business processes and administration. ICTs now routinely support the processes of decision-making, policy development and services delivery, with the consequence that the effectiveness and efficiency of a university's business processes are invariably determined by the quality of ICTs deployed as support tools. With the understanding that effective and optimum use of technological tools must be informed by standards and policies that define systematic and informed deployment, the Federal Government of Nigeria has, in the past, and through the Ministry of Education and the Computer Professional Registration Council, initiated and adopted a number of policies and regulations designed to promote the rapid but ordered advancement of the ICT sector, and exploiting its huge potential for national development. Because of the inevitability of fast technological developments and market convergence of the global ICT industry, new ICT policy frameworks are often required, and conventional wisdom is that ICT policies and regulations should be characterized by such flexibility as will enable the ready accommodation of developments in the industry.

Outcomes of a recent comprehensive survey conducted by National Information Technology Development Agency (NITDA) reveal that quite a few Nigerian universities have ICT policies of some type, but that the policies typically prescribe rules and regulations for 'appropriate' and 'responsible' use of facilities and resources, often to the exclusion of issues concerning e-learning and capacity building.

The goal of the Guidelines and Standards for ICT support services in Nigerian Universities therefore, is to provide a flexible and comprehensive general framework for the deployment of ICT tools in Nigerian universities for the effective and efficient support of the core business processes of teaching, learning, research and administration. National Information Technology Development Agency (NITDA) through the National Universities Commission (NUC) will request for the adoption and implementation of the policy by:

a) All Federal Universities and
b) All State-Owned Universities.
Standards and policies prescribed in the document are designed to serve the purposes, among others, of facilitating the ability of the target universities

✓ To provide fully automated and ICT driven business processes including records management, content delivery, and performance assessment, in Nigerian universities;

✓ To provide suitable environments for life-long learning / continuing education;

✓ To develop a methodical system of collecting and disseminating data and information of relevance to national higher education issues;

✓ To deploy efficient management information systems;

✓ To broaden the horizon of educational services provision, including medium / method of content delivery;

✓ To promote effective information exchange best practices among and between students and lecturers;

✓ To deploy / enhance learning management systems and ICTs-supported library services

✓ To promote technology literacy of all members of the community, especially for students

✓ To develop vibrant and sustainable distance education platforms, focused on national development issues

✓ To promote the culture of learning at school (development of learning skills, expansion of knowledge acquisition options open source of educational resources, etc.);

✓ To institute and sustain capacity building programs in all areas of information and communication technology

✓ To provide access to global digital libraries' resources through networking initiatives, opportunities, and collaborations

✓ To develop inter-university linkages and collaborations including content delivery with the use of Video conferencing and live video broadcast

2.0 POLICIES

These policies provisions represent guidelines that:

a. Define authorities, responsibilities and accountabilities for Information and Communication Technology (ICT) operations and management within each university;

b. Prescribe a policy framework or template with which each university can develop localized frameworks to derive maximum benefits from the usage of ICT, as informed by its circumstances
c. Specify policies for the management of ICT resources and activities and concerning the following:
   a) Software acquisition, development and usage, and maintenance;
   b) Acquisition of ICT equipment, infrastructure and services;
   c) Repairs, disposal and disaster recovery;
   d) ICT networking infrastructure development;
   e) Universal access management and control;
   f) Funding of ICT equipment and infrastructure;
   g) Data and information management;
   h) Network services - Internet, email services and university website;
   i) E-learning and digital resources;
   j) Cyber security issues - prohibited use of university's ICT resources;
   k) Enforcements.

3.0 SOFTWARE ACQUISITION, DEVELOPMENT AND USAGE

Every university can benefit tremendously by developing its own software, as this will not only eliminate dependence on non-university for the delivery of ICT-supported critical services, but will also guarantee a ready and cost-effective customization to changing needs; As virtually all Information Management processes involving staff and students are supported by various software applications. Each university should, therefore, strive to build a strong collaborative interface with local and international software industries, and as matter of policy, significantly participate in activities of various global open source software development groups.

Policy guidelines in this section extend over the following items:
   a. Software Development;
   b. Open Source Software;
   c. Pirated (or illegally acquired) Software;
   d. Operating System software;
   e. Software Uninstallation;
   f. Software Copying;
   g. Software Storage and records keeping;
   h. Software Updates and Upgrades.

3.1 Software Development

Universities are well-advised to have policies that define and prescribe processes for the development and procurement of software in a manner that increases efficiency and guarantees desired product quality assurance metrics.
Policy statements shall encourage the building of capacity for in-house development of software by setting up a well-equipped Software Engineering unit staffed with high caliber software developers. Software development and acquisition policy issues include

i) Standardization (in-house or outsourced/off the shelf)

ii) Quality assurance strategy

iii) Licensing and ownership

iv) Technical support and software maintenance

v) Software disposal

3.2 Open Source Software

The term 'Open source software' may be defined as “software that can be freely used, changed, and shared (in modified or unmodified form) by anyone very often developed and shared in a public, collaborative manner” without restrictions. When open source software is to be adopted for use with university business processes, associated policy statements shall require testing and quality assurance certifications. In addition, provisions for back end audit trails, information classification, and different user privilege levels should be required.

3.3 Pirated (or Illegally Acquired) Software

“Software piracy” refers to the unlicensed, unauthorized reproduction and illegal distribution of software, whether for business or personal use. It should a matter of University policy that:

i. All propriety software shall comply with developers/vendors licensing and ownership policy provisions

ii. No pirated or unlicensed software shall be allowed on any official University's computer systems.

iii. Members of the university community shall be encouraged to avoid the use of pirated software with personal systems

3.4 Operating System Software

i. It is useful to maintain standards for operating systems utilized in different environments for interoperability and efficient services delivery. Operating systems in common use include:
   - Windows Operating System
   - Macintosh Operating System
   - Linux Operating System
ii. All acquired operating systems (and any other software) should provisions to software maintenance support, and for upgrades, when desirable.

3.5 Software Uninstallation
In certain situations, it becomes necessary to uninstall software, which might have been deployed for critical business processes, and whose uninstallation may have consequences for data and information items, if not properly handled. It should consequently be a university policy that the uninstallation of software deployed for use with university business processes shall require formal clearance from the ICT Centre, for the purposes of ascertaining that the uninstallation will not adversely affect records or associated processes.

3.6 Copying of Software
Staff, Students and visiting staff of the University should be prohibited by policy, from making unauthorized copies of university-owned software or soft documents.

3.7 Software Storage and Records Keeping
Efficient delivery of ICT support services is significantly dependent upon adequacy of records keeping. University policy should require the ICT Centre to have responsibility for keeping records/inventory of interest to ICT related issues, including software acquisition documents (such as purchase receipts, service level agreements, user/maintenance manuals) the original CDs, and disused or archived software.

3.8 Software Updates and Upgrades
In the typical setting, the need to improve the efficiency of a software's functionality or include an additional functionality can only be met by a software upgrade. The recommended policy is that the decision to upgrade should be informed by systematic considerations, possibly provided by a committee of ICT professionals within the ICT center.

4.0 ACQUISITION OF ICT EQUIPMENT, INFRASTRUCTURE AND SERVICES

Policy provisions concerning the procurement of ICT equipment, devices, associated infrastructure, and services, should define strategies for the effective management including acquisition policy, inventory control policy, first level equipment maintenance, and technical support policy. In addition, policy provisions should cover procedures, as
well as roles and responsibilities for personnel involved. In most cases, the main responsibilities will reside with the University’s ICT Centre, whose annual budget covers equipment purchases, equipment maintenance, internet bandwidth, software licenses and backbone network maintenance. Typical policy provisions include:

i. Equipment, devices, or services shall be procured ONLY from Original Equipment Manufacturers (OEM) or accredited agents/partners.

ii. Donated ICT equipment and devices shall ONLY be accepted, if they are certified as acquired from the OEM or accredited agents.

iii. The ICT Center shall develop specifications for equipment, devices, and services, to encourage standardization and consequently ease corrective and preventive maintenance processes.

iv. Bulk purchase of parts required for maintenance activities shall be encouraged, and implemented under the supervision of ICT Center personnel.

v. Business models shall be developed to prescribe service level agreement provisions for ICT services provided by vendors and services providers.

5.0 MAINTENANCE, DISPOSAL AND DISASTER RECOVERY

Orderly and well-planned maintenance of ICT devices, equipment, and associated infrastructure is of critical importance to the quality of ICT support services that the university can expect. Policy provisions therefore should include informed guidelines for equipment maintenance, which may extend over such maintenance activities as

a. First level and routine maintenance

b. Disposal of ICT equipment, devices and software

c. Disaster Recovery and contingency plan

5.1 First Level and Routine Maintenance

The ICT Centre should have the responsibility of providing centralized technical support services for all aspects of ICT including hardware and software. In addition, the center should

i) Train ICT asset owners on how to carry out first level maintenance, as a means of reducing equipment/devices down time; and provide manuals to serve as guide.

ii) Develop and provide user manuals that will facilitate the ability of asset owners to carry out preventive maintenance activities, and hence prolong equipment life

iii) Maintain accurate records of maintenance activities on all ICT equipment and devices
5.2 Disposal of ICT Equipment, Devices and Software
The ICT Center should be required, as a matter of policy, to prescribe ICT equipment/devices replacement guidelines, including scheduled replacements, informed by pre-defined life cycle and maintenance history.

i) In the case of hardware, disposal should be in compliance with practices specified by extant policy on the disposal of public assets, as well as environmental protection laws and statutes.

ii) Disposal of software should typically be informed by support life-cycle advertised by the developer.

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, and other mission critical systems do not go down for a time beyond 24 hours. These requirements can be met with the following considerations.

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 ICT Centre shall develop data backup guidelines and make them available to all units of the University. In addition, cyber security best practices should be widely circulated to prevent against cyber-attacks, including denial-of-service and ransomware attacks.

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

v. In the case of data of interest to critical services, cloud backup should be considered.

6.0. ICT NETWORKING INFRASTRUCTURE DEVELOPMENT

ICT Networking Infrastructure offers a range of technologies to assist an organization in running effectively. In this section, the following shall be considered:

6.1 ICT Backbone Infrastructure
Best industry practices require that Universities should have a rollout plan (typically 5-year plans) as part of broader strategic planning considerations. Such plans will take account of the dynamic environments of computing needs, projected traffic growth, and technological advances. Other policy provisions should include:
6.2 Backbone Network:
- ICT Center shall at all times, have updated versions of the University-wide enterprise architecture, and shall be responsible its development and maintenance
- New technology shall only be introduced after professional tests confirm conformity with standards and performance requirements.
- Standards for structured cabling, as prepared by the ICT Center, shall be updated from time to time, and enforced across the university.

6.3 ICT Project Management
Every University should naturally be committed to continuously improving the delivery of ICT driven and supported services, within an approved budget, and using competent and qualified personnel. Well designed and managed ICT projects should further the objectives of effective and efficient services. ICT projects management policies should consequently include the following provisions:

i. Assignment of responsibility for the implementation of ICT projects to the University management through the ICT Centre.

ii. Oversight functions to ensure that procedures conform to the University rules and regulations possibly through the constitution of Project Implementation Team (PIT) with membership including Director of the ICT Centre, Dean/Head/Director of the direct beneficiary faculty/department/directorate of the project, where applicable.

iii. Detailed functional and technical specifications must be documented and signed off by the Project Sponsor and the Director of ICT Centre.

iv. All completed ICT projects shall be formally handed over to the ICT Centre after ensuring that adequate training and documentation, as may apply, have been provided.

7.0 ACCESS MANAGEMENT AND CONTROL

The University shall explore every ICT potential so as 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 University systems and applications to protect the privacy, security, and confidentiality of University information assets and systems. Access control may be regarded in two dimensions; namely, access to physical facilities and university buildings; and access to computing infrastructure and ICT services. A responsive ICT policy should provide for smart access to such university buildings and facilities (Library, Hostels, ICT Center, etc.) as are not ordinarily open to the general public.
Policy considerations concerning access to University computing facilities should cover:

a. ICT Infrastructure 
b. Network Control and Cyber Security 
c. Operational Environment

7.1 ICT Infrastructure
ICT infrastructure consists of three major components:

a. The data communication network (DCN) 
b. The network operations centre (NOC) 
c. ICT services and computing resources for users

7.1.1 Data Communication Network (DCN)
The data communication network includes all equipment and devices that facilitate the transmission and routing of data communication information items to various destinations across the university. Important policy provisions for the DCN include:

i. Management of all associated infrastructural components, which is typically the responsibility of the ICT Center

ii. Hosting of Domain Name Services (DNS) and servers, a responsibility of the ICT Center

iii. Provision of redundancies for core network components to ensure uninterrupted services

iv. Ownership of IP number space as prescribed by AFRINIC

7.1.2 Network Operations Centre (NOC)
Network Operations Centre (NOC-or 'Data Center') is the home for all production servers and ancillary equipment that provide the hardware platform for the central network services of the University. Industry best practices prescribe the following policy provisions:

i. Access to the NOC and network installations shall be secured and available ONLY to authorized personnel.

ii. All NOC equipment shall be labelled in accordance to a pre-specified scheme approved by Management

iii. The ICT Center shall keep an up-to-date inventory of all NOC equipment and devices, including maintenance schedules and maintenance history

iv. Standards shall be specified for ICT equipment installed on the University network, and authorized installations shall comply with the standards.

v. The ICT Center shall in collaboration with the University's Legal Unit, define
Service Level Agreements (SLAs) for use with the management of services provided by Third Party Services Providers including ISPs and other ICT services.

vi. Access to NOC facilities by contractors or other Third Party shall with the authorization, and under the supervision of ICT Center personnel.

7.1.3 ICT Services and Computing Resources for Users
In addition to ICT services, the University is obliged to provide computing resources, such ICT equipment (computers and related accessories) that the University community uses to access the various network services and for computer-based-examinations. Associated policy should provide for:

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

ii. ergonomic correctness of access facilities to prevent against any negative physical or physiological impact or damage to users.

iii. secure e-mail services, with well-defined quotas, under the management of user account managers, with responsibility of assigning accounts, enforcing use rules, and periodically reviewing performance.

iv. optimization of bandwidth utilization through the establishment and institution of an efficient cache management regime

v. a secure, effective, and efficient intranet and associated web portal

vi. rights by university authorized personnel, to audit any device attached to the university's network, without serving prior notice.

7.2 Network Control and Cyber Security
Network control and cyber security 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. The main policy objective in this case, is to protect University digital assets (including information assets) against denial of availability, compromise as well as breaches of confidentiality and integrity. And accordingly, policy provisions should include:

7.2.1 Assignment of Roles and Responsibilities
- Committee of Senate or Council to assume ownership of all cyber security risks and elucidate the University's information risk avenues
- The ICT Center, whose responsibilities shall include
  i. Instituting appropriate security controls and mechanism as informed by
risk assessment outcomes; and maintaining an up-to-date risk register.

ii. Development and utilization of a periodic systems and infrastructure audit, with basis in 'PDCA (Plan, Do, Check and Act)' cycle.

iii. Instituting an effective mechanism for the control and auditing of user privileges, including administrative privileges

iv. A continuous monitoring, in real time, of all ICT network devices, and keeping records of outcomes of the analysis of security logs

v. Implementation of industry-standard protection mechanisms for the protection of wireless access services

vi. Regulation of access to ICT resources, enforcement of acceptable use policy, and deployment of associated standard security mechanisms and technologies.

vii. Developing and maintaining accounts and privileges management procedure, including handing over of equipment/devices, schedules, and privileges in the event of disengagements or transfers.

7.2.2. Unacceptable Use of Resources
This policy provision specifies uses and practices that are prohibited, and include the following:

i. Sharing of personal pass phrases or passwords

ii. Use of pirated and unauthorized peer-to-peer software on university computing systems or devices

iii. Uses or actions that infringe on copyright and intellectual property rights

iv. Practices that have potentials for disrupting the normal functionality of university computing system or network

v. Introducing malware or malicious software into the network

vi. Improper or immoral use of facilities including paid advertisements, Peer-to-Peer File Sharing (P2P), Business activities, pornography, Gambling, Computer Games. The ICT Center's networking team shall 'gray out' known sites, and continuously update the lists of sites offering the offensive services for blacklisting.

7.2.3 Antivirus
These are software utilities that protect the computers and networks from maliciously introduced applications and various malware types. Malware protection policy provisions include:

i. availability of protective antivirus software designed to detect, remove and defend
all University computers against malicious software, malware or viruses.

ii. subscription to services of reputable malware protection services providers for the provision of enterprise-wide, real time protection.

iii. Guidelines for computer virus management across the university

7.3 Operational Environment
This refers to the environment within which the ICT equipment is installed and operated. The typical working environment for all ICT facilities should have the following provisions:

a. Uninterrupted Power supply
b. Adequate and well-maintained air conditioning system
c. Illumination
d. Fire protection - detectors and extinguishers
e. Cleaning tools

7.3.1 Uninterrupted Power Supply
This should consist of a suitable combination of the following

a. Public power supply;
b. Standby generators;
c. Battery banks or inverters of adequate capacity (especially for centralized systems)
e. Stabilizers and power surge protectors;

7.3.2 Adequate and Well-Maintained Air Conditioning System
Air conditioning systems provides cooling that keeps the operational environment of the ICT facilities within the equipment manufacturers' recommended specifications for temperature and humidity all year round with the aid of humidity detector (Hygrometer/Psychrometer).

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

7.3.3 Illumination
This is a device that provides illumination.

The University shall ensure that the computer facilities are provided with functional lighting systems that operate at all times.

7.3.4 Fire Protection - Detectors 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.

7.3.5 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 – free 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.

8.0 FUNDING OF ICT EQUIPMENT AND INFRASTRUCTURE

ICT projects are necessarily capital intensive. The design, establishment and management of ICT projects require a lot of funding and financial processes. These finances are typically sourced, both internally and externally. Policies on funding ensure systematic sourcing and consequently, continuous availability of funds. The associated provisions extend over

a. Source of funding for ICT equipment and infrastructure

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 ICT CENTRE 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 Vice Chancellor;

   i. The University shall create a separate ICT budget annually for ICT funding.
   
   ii. The ICT budget votes shall have specific provisions for:
         \ Hardware acquisition
         \ Software license fee
         \ Hardware maintenance
         \ System Development
         \ ICT Technical Staff Training
         \ ICT user training
         \ ICT staff salaries
         \ Equipment spares
         \ Communication Fees (Bandwidth servicing)

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 will have its local database. It shall also adopt a backup at the Central Storage which shall be managed by the ICT Centre.

ii. The ICT Centre shall ensure that each Unit/Department shall work out their own Data Security details.
9.2 Data Confidentiality
i. Authorized Users shall keep confidential record of all the 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 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. University Website
e. Disclaimer

10.1 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 ICT Centre.
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 users 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.

10.2 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 ICT Centre.
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.

10.3 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. University e-mail account
   b. Closure of University e-mail account
   c. Mailing lists

10.3.1 University E-mail Account
University e-mail service is available for all staff and students under the official
University domain name (University.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 University 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 University's e-mail account.
      vi. All official correspondences and public interaction shall be via the
          University'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 University'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 University e-mail domain.
• Attachments sent are virus-free.

10.3.2 Closure of University E-mail Account
i. The University 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 University 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

10.3.3 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 Vice Chancellor, Registrar, statutory boards, committees and others as approved by the Vice Chancellor or Registrar
10.4 University Website

It is the policy of the University to have an official website (University.edu.ng) that showcases the University to the rest of the world for the purpose of 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 University 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 University website as a quick and easily accessible means of communication with the University's target audience.

Some other considerations are listed below:

i. University web pages are the primary entrance points to the University's website and the appearance and content shall be the responsibility of the ICT Centre.

ii. The ICT Centre 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 ICT Centre 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 Vice Chancellor.

10.5 Disclaimer

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

11.0 E-LEARNING AND DIGITAL RESOURCES

This is refers to 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

11.1 E-Learning Resources
i. The University shall acquire a versatile e-learning platform (open source or propriety) for use with e-learning activities. All university Faculties and teaching units should be enabled to effectively utilize the platform for content delivery learning and information exchange.

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 ICT Centre 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. The university shall 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.

11.2 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.

The university community should note the following:
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 (Electronic Document Management System-EDMS Unit) of the ICT Centres.

11.3 Digital Preservation Archiving

The rapid growth in the number of digital resources and the University's budget used to obtain them has made it necessary 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 University Library's expanding digital collections.

ii. University 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. The University 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. The University library shall commit to ongoing 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. University 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 the University 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 University 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 ICT centre 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.

11.4 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 the 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 the operation of this policy, be subject to a perpetual non-exclusive, 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 research, education and development in the University. This office shall also provide guidance regarding a 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 will be 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 shall have to consult with the appropriate office regarding such matters.

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

11.5 University Library

i. In terms of ICT services, the University Library, supervised by the ICT Centre will be responsible for creating and making available electronic-based library information resources for the purpose of teaching, learning and research. These will 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.

11.6 Capacity Building/ End-User Skills Development
Use of ICT-supported and ICT-driven business processes invariably requires training in order to ensure effective and efficient utilization of resources. The effectiveness of training programs will depend on informed identification of training needs, which in turn, can be achieved through adequate ICT policy provisions. Such provisions include:

i. mandatory training in basic and essential ICT skills for all cadres of staff and students

ii. programs for the continuous training for ICT personnel, as informed by periodic skills assessment to identify knowledge gaps

iii. regular programs for training and ICT-driven skills acquisition and improvement for teaching staff and facilitators at all levels

vii. development of capacity building modules for use with training programs and designed to address specific ICT skills gaps.

viii. Building a pool of instructors (in-house and external experts) for training programs

ix. facilitating the ability of the ICT Centre to conduct skills assessments and consequently recommend ICT training as may be indicated by skills assessment outcomes

x. capacity building and collaboration programs designed to enable significant self-reliance

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

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

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

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

iv. The ICT Centre 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 ICT Centre 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.
Sources of this materials utilized include the following:


b) The Council of Computer Professionals Registration Council of Nigeria, in accordance with the Statutory Provisions of Section 17; see https://lawsofnigeria.placng.org/print.php?sn=78

