NNAMDI AZIKIWE UNIVERSITY AWKA

ICT POLICY AND GUIDELINES

The Information and Communication Technology (ICT) Policy and Guidelines Document, is a statutory Instrument of the University for reference by Staff, Students and Visitors.

Approval
By

____
Vice-Chancellor

Date ______________24/03/2023_______________________

TABLE OF CONTENTS

DEFINITIONS

ICT

Acronym for Information and Communication Technology. Examples are, Software, Hardware, Web Applications, Database, Network and Internet services.

ICT Policy and Guidelines

A formal document adopted by the constituted authority, detailing principles, plans and procedures to guide all and sundry on ICT utilization.

ICT Infrastructure/Resources

This refers to all of the University's Information and Communication Technology Resources and facilities including, but not limited to: desktop computers, Laptops, printers, scanners, access labs or other facilities that the University owns, leases or uses under Licence or by agreement, any off campus computer and associated peripherals and equipment provided for the purpose of University work or associated activities, or any connection to the University's network, or use of any part of the University's network to access other networks.

Management Information and Communications Technology Unit (MICTU)

The Management Information and Communications Technology Unit is the hub (i.e. coordinating unit) for all ICT activities. It is a statutory organ of the University vested with the authority to develop, deploy and manage all ICT infrastructures and resources, certify all ICT supply and services within the University, and to ensure that, the provision of ICT infrastructure and services are aligned with the University academic and administrative direction and priorities.

The University

Refers to Nnamdi Azikiwe University, Awka

INTRODUCTION

In today's educational system, and particularly the tertiary education, ICT has become a universal tool to reckon with, for the enhancement of academic and administrative processes, going forward therefore, the University will rely on the integrity and availability of its Information and Communications Technology (ICT) infrastructures/resources to meet needs and to ensure effective communication and working practices. Improper use of the University's ICT infrastructures can impact adversely on the institution, waste time and resources, create legal liability and embarrassment for both the University and the user, thus sanctions are prescribed for offenders and abusers of the institution's cyberspace.

AIM

We aim to create a platform which will enhance the productivity and outputs of both staff and student, provide an enabling and limitless environment that enhances creativity and innovation among students and staff. In doing so, we shall;

1. Provide a robust, flexible and reliable ICT infrastructure and an information governance framework to support and sustain excellent research, learning and community services.

2. Provide prompt ICT technical support, guidance and training to our research community, draw up governmental, research and learning network aimed at meeting the mandates of the institution.

3. Regularly engage with staff, students and the research community and keeping them updated on developments and changes in ICT as it applies to their areas

4. Provide high quality, centrally controlled custom made secured and reliable access to all ICT platforms and services that supports research, learning and community development.

5. Segregate our ICT service providers, suppliers, vendors and contractors according to their relevance to our institutional goals and identify additional ICT services and enhancements that can be delivered in line with our mandate.

6. Provide dynamic, expandable and secure platform and an information governance system aimed at supporting and sustaining excellence in teaching, learning and research so that institutional requirements and personal goals are met.

This document does not form part of the contract of any employee and the University reserves the right to alter or amend this policy at any time.

Responsibility

The University through the Committee on Information Communication Technology (ICT) has overall responsibility for this policy, including keeping it under review while staff, students and visitors have responsibility to comply with the terms of this policy. Therefore, any queries regarding this policy or ways in which it might be improved should be directed to the ICT Committee.

ICT Policy Vision Statement

To enable research, teaching, learning and community development and boost the digital experience to achieve the vision of the University through provision of viable and reliable ICT solutions.

ICT Policy Mission Statement

To ensure a process of responsibility and accountability for the integration and utilization of viable and reliable ICT infrastructures/resources, with innovations in teaching, learning, research and Information Systems for business processes, in line with the mission of the University.

Objectives of the ICT Policy

The overall policy objectives are:

1. To ensure that, procedures and guidelines for selection and use of ICT facilities in the University are adhered to by staff, students and visitors alike.

2. To employ effective governance structures, to establish and develop ICT infrastructure for optimal utilization in core businesses.
3. To produce ICT literate students and enhance ICT literacy among members of staff.

5. To empower our students, staff and visitors with ICT skills in line with global digital trend.
6. To protect the University from any legal implications arising from unethical use of the University's ICT infrastructure.

Significance of the ICT Policy

The establishment of the ICT governance structures will allow key principal administrators to be carried along and be well informed about the status and challenges of ongoing ICT projects, so that budgetary, timelines and deliverables are synchronized, significant technology-related risks are addressed, so that the use of the University ICT resources/infrastructures are optimized. Hence, it will bring about consistency in the support and implementation of ICT Development plan and prioritized ICT projects in the current and subsequent administrations.

Also, with the teeming increase in the use of electronic communication in present day realities, it is essential that the University protects its resources from illegal, defamatory, fraudulent or other misuse. This policy contains guidance on the measures that must be taken by staff, students, workers, contractors, and any other users to ensure that the University's ICT resources/infrastructures are adequately secured and appropriate standards are met. It also outlines when the University will monitor the use of its ICT infrastructures/resources in order to checkmate misuse or unauthorized usage.

Coverage

This policy document applies to all students and members of staff of the Nnamdi Azikiwe University; ICT vendors, contractors, visitors, researchers and all users of the University's ICT infrastructures/resources.

Electronic Communications (Emails)

For every operation, whether virtual or physical, all official communications or information can either be by hard copy, university e-mail or by electronic memo.

1. The University's e-mail service is available for all staff and students under the official institution name (unizik.edu.ng) governed by this ICT Policy.

2. Users shall be required to have a University e-mail account which will be issued after approval by the authorized officer of the Management Information and Communication Technology Unit. (MICTU).

3. E-mail shall be an acceptable means of disseminating official information (internal memos, notices and the University bulletin) throughout the University community.

Users are not allowed to:

a. Use institution's e-mail account for spamming;

b. Use unethical languages in e-mails;

c. Falsely represent the University's assert or imply that personal views or opinions are the University's view or opinion;

d. Use the e-mail account for any commercial purpose;

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

f. Use the e-mail account for disseminating offensive materials that may offend the ethnic, religious or gender sensitivity of others

g. Use the e-mail account for propagating negative impressions against the University's management;

Users are expected to:

a. Ensure that their access information (username and password) are kept private and promptly report to the designated officer of MICTU in cases where compromise is suspected.

b. Be accountable for any e-mail sent using their account.

c. Ensure that the confidentiality and privacy of official information is upheld and official information is not circulated beyond the boundary of the University e-mail domain;

d. Ensure that attachments sent are virus-free.

Deactivation of University E-mail Account

The University e-mail account of staff shall be deactivated or disabled if the staff is dismissed, Resigns, retire or dies.

The University students' e-mail account shall be deactivated or disabled if a student graduates, is dismissed, suspended or dies.

The University's Monitoring Rights

The University reserves the right to monitor telephone, email, voicemail, web and other communications traffic for institution reasons, and in order to perform various legal obligations in connections with our role as an institution. The use of the University's ICT infrastructures/resources including the computer systems, and any personal use of them, is continuously monitored.

Monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for education purposes. The University reserves the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is non-exhaustive).

1. To establish facts relating to the institution (e.g. whether a contract has been entered into over the telephone/ email)
2. To ascertain compliance with regulatory practices
3. To ascertain whether standards are being achieved by persons using the system – this will include quality control and staff training
4. To prevent or detect crime
5. To investigate or detect the unauthorized use of the University's ICT systems
6. To ensure the effective operation of the system, e.g. checking for incoming computer viruses etc.

Nnamdi Azikiwe University has an official website (unizik.edu.ng) that showcases her to the world through the disseminating of up-to-date information from all organs of the institution, Faculties, Colleges, Departments, Directorates, Centres, Institutes and Units.

The website provides necessary information about the functionality of the University, curriculum, events and general information of the University community. The website will amongst other things:

1) Enhance the University's presence on the internet and broaden its recognition, while strengthening its image;

2) Publish current and informative content in a generally acceptable manner;

3) Support a sustainable information and communication infrastructure that supports the University's mission, goals and objectives through an on-line presence;

The Nnamdi Azikiwe University web pages are the primary entrance points to the University website, hence the appearance and content shall be the responsibility of the MICTU.

MICTU 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 / bulletin and ensure that the content of the site conforms to the mission and mandate of the University.

Each Faculty/Department/Directorate/Unit/College shall setup a committee to provide information to their respective ICT officers for update on the web pages.

No Unit/Faculty/Department/Directorate/Unit/College shall be allowed to host their own website or web- pages outside the University's web server. Where this is deemed necessary, permission shall be sought and obtained from the Vice Chancellor.

VIRTUAL OPERATIONS

Meetings, lectures, examinations, seminar, researches, conferences etc. may be held and conducted virtually via Zoom, Microsoft Teams, Whatsapp, Skpe, Google meet, Teamviewer, or any other virtual App.

Where meetings, lectures, examinations, conferences, seminars etc are to be held and conducted virtually and in real time, authorized MICTU staff shall put in place adequate mechanisms to enable seamless operation, activities, functions or meeting.

WORKING FROM HOME

Authorized Users with administrative access may be allocated with a laptop computer to allow them to work from home and/or certain Users maybe require on occasions to use their own computer at home to undertake assignments. Such Users should ensure that unauthorized software are not installed on University laptops. Users working from home should take extra care when receiving or downloading information to make sure that such information is virus free.

Any user wishing to take files on storage sources to work on their home computer should ensure the following before doing so:

1. A copy of the file is on the University's server as a backup.
2. The storage source is not left in any place where it might be stolen or copied.
3. The storage device is scanned for virus (es) before and after copying data onto it.

VIRUS CONTROL

All Users must act in accordance with legislation and good practice to ensure that at all times the integrity of software and data is safeguarded. For the integrity and availability of IT services to be maintained precautions are required to prevent and detect the introduction of computer virus. Remember: **UNAUTHORIZED COPYING OR DISTRIBUTION OF SOFTWARE IS A CRIMINAL OFFENCE.**

HEALTH AND SAFETY

To ensure the health and safety of users in so far as is reasonably practicable, the University will in consultation with Users:

1. Assist in conducting analysis of display screen equipment workstations, assessing the associated risks and applying appropriate control measures.
2. Provide suitable and sufficient training and information on the safe use of display screen equipment, including University safe work routines and awareness of the symptoms of work related upper limb disorders.
3. An eye sight test is recommended annually.

4. Review software as necessary to ensure that it is suitable for the task, understandable and easy to use.

CONFIDENTIAL INFORMATION

Users should not use University’s ICT infrastructure to disclose unauthorized confidential information, trade secrets, patents and other restrictive documents which either belong to or is the property of the University or its subsidiaries, client, contractor consultant or any third party. For clarification, staff, students, contractors/vendors and visitors should not:

1. Divulge any confidential information that they may have access to in the normal course of their employment or business or transactions with the university.

2. Seek access to data that is not required as part of their duties as a staff member of the University or

3. Store the University data on personally owned devices or any other device not owned by the University where such device can be used by another person, unless such devices are locked down to the staff member via password, pin or biometric access and the device locks itself after no more than 5 minutes of inactivity

Misuse or excessive use or abuse of our ICT systems or inappropriate use of the internet or email in breach of this policy will be dealt with in accordance with our Disciplinary Procedure, misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting, uploading or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct;

1. Pornographic material (that is, writings, pictures, films, video clips of a sexually explicit or arousing nature);
2. Offensive, obscene, or criminal materials or materials which are liable to cause embarrassment to the University;

3. A false and defamatory statement about any person(s) or institution(s) or organizations;
4. Material which is discriminatory, offensive, derogatory or may cause embarrassment to others;
5. Confidential information about the University and any of its staff, students or visitor;
6. Any other statement or information which is likely to create any liability against the University (whether criminal or civil) or to portray the University, staff or student in a bad light;
7. Material in breach of copyright laws of the Federal Republic of Nigeria;
8. Online gambling; or extortion. (this list is not exhaustive)

Any staff, student or user of the University's ICT facilities found guilty of such action, or in conspiracy or aiding/abetting anyone, will be punished accordingly. Where evidence of misuse is found, the University may undertake a detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records of such defaulting user. Where it is established that the defaulting user may have committed a cybercrime or any criminal offense, he/she may be handed over to the Police or any other law enforcement agency for criminal investigation and possible prosecution.

LIABILITY

All users of the University's ICT facility and cyberspace will be personally liable for offenses committed while using such facilities or connected to the University's cyberspace. The University's files including internet files and e-mail messages may be disclosed for the purposes of legal action.

DISCIPLINE

Users are reminded that misuse of the University's ICT infrastructure is a SERIOUS MISCONDUCT. Staff and Students who violate this policy will be subjected to the University's Disciplinary Procedure for gross misconduct. Other Users who violate this policy will be subject to appropriate action and sanction by the University. Users employing the University's ICT infrastructure for defamatory, illegal, fraudulent or malicious purposes may face civil litigation or criminal prosecution.

DATA STORAGE AND INFORMATION MANAGEMENT

All University 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 Management Information Communications and Technology Unit (MICTU).

1. Data Storage- the University shall adopt a Centralized/Distributed database system of storage where each Unit/Department (through their respective ICT officers) will have its local database. The Units/Departments shall also maintain a backup at the data storage centre which shall be managed by the MICTU. The MICTU shall ensure that each Unit/Department shall work out their own data security details.

2. Data Confidentiality - Authorized Users shall keep confidential record of all University data and information provided in confidence to the University by other entities. Each staff member is under the obligation not to disclose the University's data and information unless authorized to do so. Data and information shall be disseminated on a need-to-know basis and shall not be divulged to unauthorized persons. Breach of confidentiality through accidental or negligent disclosure shall result in disciplinary action taken against the user.

3. Data Ownership - All information acquired or created by users while carrying out the University's business, except that which is specifically exempted as private or personal, shall be owned by the University. Each User Department shall have individual ownership of its own data resource and ensure that the data is accurate and backed up regularly.

DATA STORAGE CENTRE

There shall be a data storage centre within the University premises which will house all University's ICT data, Information and records. All ICT data whether developed/generated in house or out sourced must be stored/backup at the data storage centre. A back up and recovery plan shall be activated in the event of anticipated or unanticipated loss or damage to data stored at the storage centre.

MICTU STAFF REMUNERATION CLAUSE

This clause covers all invention made by staff in the course of employment (with the University's cyberspace and facility) or the performance of specified work as specified under the Patents and Designs Act 2004 Laws of the Federation of Nigeria;

1. The right to apply for a patent in the invention is vested in the University.
2. Where the invention is of exceptional importance the MICTU staff is(are) entitled to fair extra remuneration taking into account his salary and the importance of the invention, this entitlement cannot be modified by contract and may be enforced if need be.

The University through the ICT Committee has the responsibility for ICT research and development, hence proposals for software automation technologies must be approved by the ICT Committee after due diligence has been carried out by the Management Information Communications and Technology Unit (MICTU). It is therefore expected that prospective ICT contractors submit their proposals and demo to the Director (software) MICTU for certification. Once certified, the proposal must be presented to the ICT Committee for deliberations and approval.

Use of ICT-supported processes borne from research and development invariably requires training in order to ensure effective and efficient utilization of resources. Therefore the University in consultation with the ICT Committee and the Management Information Communications and Technology Unit (MICTU) will approve:

1. Mandatory training in basic and essential ICT skills for all cadres of staff and students;
2. Programs for the continuous training for ICT personnel, as informed by periodic skills assessment to identify and bridge knowledge gaps;

3. Development of capacity building modules for use with training programs, designed to address specific ICT skill gaps;

[

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

THE ICT COMMITTEE

Purpose

To ensure that key principal administrators, are well informed about the status and challenges of ICT infrastructures and services of the University and that the use of the University ICT resources is optimized in line with the vision and mission of the University.

Mandates

The Committee shall be saddled with the following mandates:

1. Support the development and implementation of ICT Development Plan.
2. Review major ICT projects and discuss concerns (i.e. status and issues).
3. Advice the University on a sustainable, institutional funding model for ICT infrastructure and services.
4. Ensure that ICT projects are completed and delivered within stipulated timelines by the contractor.
5. Ensure through the Management Information and Communications Technology Unit **(**MICTU) (as the coordinating unit) that ICT projects attained the University's requirements, standard and specifications, and best practices prior to completion and upon delivery.
6. To ensure that all ICT supplies and services are certified by the Management Information and Communications Technology Unit (MICTU) of the University.
7. Ensure adequate staff training and technology transfer for projects executed by third party.
8. Consider any other item as directed by the Vice Chancellor.

Composition of Members

The ***ICT Committee*** shall be constituted and chaired by the Vice Chancellor or Ag. Vice Chancellor. Alternatively, the Vice Chancellor could appoint the Deputy Vice Chancellor Admin (DVC Admin) as the Chairperson. The committee shall report through the chairperson to the Vice Chancellor. However, in the event that, the offices of the DVCs are vacant, then the Vice Chancellor could appoint any high ranking staff of his choice to preside over the committee.

The ICT Committee shall consist of:

- The Vice Chancellor, as Chairman
- The DVC Admin
- The Registrar/ Representative
- The Bursar/ Representative
- The Director, Academic Planning
- The Director, MICTU (Software and Hardware)
- The PRO
- The SAVC (ICT)
- A legal personnel
- A secretary
- Ad hoc members (from within or outside the University), as required, who are experts of a particular business processes or technology.

The committee will evaluate inputs received from individuals or groups, Units, Departments and Faculties on ICT matters and make recommendations to the Vice Chancellor.

POLICY REVIEW AND AMENDMENT

This policy is to be reviewed after every five (5) years by the University's ICT Committee, however amendments can be carried out depending on the needs of the University and future modifications of ICT systems.