



**FEDERAL UNIVERSITY OF TECHNOLOGY,
OWERRI, NIGERIA**



**INFORMATION AND COMMUNICATION
TECHNOLOGY POLICY**

February 2023

The Federal University of Technology, Owerri is made up of a number of Schools, Research Centres and Institutes of Studies that are engaged in research, invention, innovations and generation of new knowledge in line with its motto “**Technology for Service**”.

The vision statement of the current University Management as encapsulated in our mantra “Driving the Culture of Excellence” is the sustenance of the application of a sound and robust ICT policy in the University service delivery, as an indispensable aid towards the achievement of the University’s unique mandate. The fulfillment of this noble vision requires a sound ICT policy that will guide the University in this critical aspect of its mandate. Hitherto, this important document is non-existent in the University.

It is important to note that the decision of the University administration to articulate and produce a robust and sound ICT policy document is to say the least, a welcome and plausible development. The adoption and implementation of the policy will significantly enhance the popularity, visibility of FUTO and hence a better **webometric** ranking.

The importance of ICT in innovation for knowledge generation and technology transfer geared at enhancing national development as a component of education for life has been embraced in the strategic plan of the University.

All existing users of ICT in the University will be informed of this policy and any future amendments to it. Continued use of ICT after notification constitutes acceptance of, and agreement to the policy document.

New students to the University will be informed of the policy at the time of orientation. Future staff will be given the policy when they join the University.

Violations of this policy will be handled in accordance with the University’s disciplinary procedures. Where necessary, violations may be referred to law enforcement agents for prosecution.

This policy does not attempt to anticipate every situation that may arise and does not relieve anyone of their obligation to use common sense and good judgment.

For the effective implementation of this policy, the University shall constitute a **FUTO ICT COMMITTEE** to support the realization of the objectives of the policy and ensure its compliance. The Committee will also have a clear mandate to develop new operational codes and guidelines in line with international standards and protocols.

It is therefore my desire to present this ICT Policy document to provide the needed guidelines for administrative, teaching, research activities and support services by staff and students of the Federal University of Technology, Owerri.

Prof. (Mrs) Nnennaya N. Oti
Vice-Chancellor

Contents

	FOREWORD -	-	-	-	-	-	-	-	-
1.0	INTRODUCTION	-	-	-	-	-	-	-	-
2.0	VISION	-	-	-	-	-	-	-	-
3.0	MISSION	-	-	-	-	-	-	-	-
4.0	PHILOSOPHY	-	-	-	-	-	-	-	-
5.0	POLICY OBJECTIVES	-	-	-	-	-	-	-	-
6.0	UNIVERSITY WEBSITE	-	-	-	-	-	-	-	-
6.1	Support of University Website	-	-	-	-	-	-	-	-
6.2	Plagiarism Check	-	-	-	-	-	-	-	-
6.3	Copyright and Limitation of Liability	-	-	-	-	-	-	-	-
6.4	Warranties	-	-	-	-	-	-	-	-
6.5	Changes	-	-	-	-	-	-	-	-
6.6	Disclaimer	-	-	-	-	-	-	-	-
7.0	THE EDUCATIONAL PORTALL AND OTHER INFORMATION SYSTEM	-	-	-	-	-	-	-	-
7.1	The Educational Portal	-	-	-	-	-	-	-	-
7.2	Online Admission Application System	-	-	-	-	-	-	-	-
7.3	Online Payment System	-	-	-	-	-	-	-	-
8.0	NETWORK DEVELOPMENT AND ICT INFRASTRUCTURE	-	-	-	-	-	-	-	-
8.1	Departmental/Unit ICT Infrastructure	-	-	-	-	-	-	-	-
8.1.1	Laptops, Ipads and Tablets	-	-	-	-	-	-	-	-
8.1.2	Computing Facilities and Internet Services	-	-	-	-	-	-	-	-
8.1.3	Specialized Computing Requirements	-	-	-	-	-	-	-	-
9.0	POWER SUPPLY AND EQUIPMENT PROTECTION	-	-	-	-	-	-	-	-
9.1	Power Supply	-	-	-	-	-	-	-	-
9.2	Equipment Protection	-	-	-	-	-	-	-	-
10.0	TRAINING AND CAPACITY BUILDING	-	-	-	-	-	-	-	-
11.0	SOFTWARE ACQUISITION AND DEVELOPMENT	-	-	-	-	-	-	-	-
11.1	Software Acquisition	-	-	-	-	-	-	-	-
11.2	Software Development	-	-	-	-	-	-	-	-
12.0	LIBRARY INFORMATION SYSTEMS	-	-	-	-	-	-	-	-
13.0	HUMAN RESOURCE INFORMATION SYSTEMS	-	-	-	-	-	-	-	-
14.0	E-LEARNING AND SUPPORTING STRUCTURE	-	-	-	-	-	-	-	-
14.1	LEARNER SUPPORT	-	-	-	-	-	-	-	-

15.0	IT SUPPORT, BACK UP/RECOVERY AND HELP DESK	-	-	-	-
15.1	IT Support				
15.2	Backup/Recovery	-	-	-	-
15.3	Helpdesk Software	-	-	-	-
16.0	PROCUREMENT AND MAINTENANCE OF ICT INFRASTRUCTURE AND SYSTEMS				
17.0	DISPOSAL OF OLD COMPUTERS & LIFE CYCLE REPLACEMENT OF COMPUTERS				
16.1	Disposal of Old Computers	-	-	-	-
16.2	Importance of Data Removal	-	-	-	-
18.0	ACCEPTABLE USE	-	-	-	-
19.0	UNACCEPTABLE USE	-	-	-	-
19.1	Infringement	-	-	-	-
20.0	POLICY IMPLEMENTATION AND RESPONSIBILITY	-	-	-	-
21.0	ABBREVIATIONS	-	-	-	-
22.0	DEFINITION OF TERMS	-	-	-	-
23.0	DOCUMENT SCOPE, CONTROL AND REVISION	-	-	-	-

FEDERAL UNIVERSITY OF TECHNOLOGY OWERRI

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

1.0 INTRODUCTION

Information and Communication Technology (ICT), is the convergence of computer technology, telecommunication and electronics. Advances in ICT, namely; Internet, mobile phones, data communication, satellite television, smart devices, have provided an unprecedented productivity increase in organizations. Consequently, most businesses in the world today, depend on ICT, Teaching, learning, research and administration in tertiary institutions, presently cannot be effectively carried out without the use of ICT.

In furtherance with the administration's mantra of "Driving the Culture of Excellence", this ICT policy document has been designed to ensure that the University's ICT facilities are well utilized, managed and protected. This Policy shall apply to all University staff, students, parents, contractors, service providers and other relevant stakeholders. This policy will serve alongside the University ICT Roadmap, Strategic Plan and any other related published document, as the reference document on ICT use and development.

2.0 VISION

To use ICT tools to re-position FUTO into a world class University of excellence in teaching, learning, research and development.

3.0 MISSION

To promote the increased use of the state-of-the-art ICT hardware and software resources that will improve and sustain the productivity of FUTO students and staff to international standard at all times in areas of Students Laboratories, Applications Development, Teaching & Research, Staff Training and Consultancy.

4.0 PHILOSOPHY

The philosophy of this Policy is to have a document to guide the use of ICT infrastructure and development, for optimal benefit to the University community and mankind.

5.0 POLICY OBJECTIVES

To realize the vision and mission, the University has set the following objectives:

- i. Sustenance of the University Website and Educational portal for all academic business processes.

- ii. Provision of a working environment that encourages access to knowledge and sharing of information by putting in place, computers in staff offices and laboratories and dedicated bandwidth for academic purposes.
- iii. Development and sustenance of wired and wireless reliable campus-wide network to facilitate access and sharing of data.
- iv. Promotion of widespread use of ICT for efficient teaching and learning through training workshops for staff and students.
- v. Setup of appropriate mechanism for digitization of the University's historical data and information; Students' records, University archives, Inventory, Bursary and Human Resource (HR) Information.
- vi. Sustenance of the computerization project and the quest for excellence in paperless office procedures: student's admission, transcript processing and other student services.
- vii. Provision of a commensurate annual budget for replacement/maintenance of ICT infrastructure for expected benefit realization.
- viii. Establishing of ICT Committee/quality Control and Assurance team for ICT.
- ix. Adoption of Federal government and National Universities Commission's ICT projects/programs on E-learning, & Nigerian Research and Education Network (NgREN),
- x. Adoption of relevant standards on ICT use in academic environments.

6.0 THE UNIVERSITY WEBSITE

The purpose of the University Website is to access official University information, to disseminate and extend knowledge and to foster the free exchange of ideas. It is also a valuable asset for marketing and branding the University, and for reaching and engaging key stakeholders.

The content of the University's website will be used to uphold the integrity and image of the University. All University software applications for students, alumni and potential students shall be accessed through the University Website.

6.1 Support of University Website

The University Website is responsible for the design, development, maintenance, and oversight of the Website of the Federal University of Technology, Owerri. The University Webmaster will only publish information approved by the Vice-Chancellor or her designate.

The Webmaster serves as the Campus expert consultant on web publishing and the use of new technologies and innovations in the area of web development. Under the supervision of the Director, ICT Centre, the University Webmaster will work closely with academic Departments, administrative offices and student

organizations to ensure the availability and professional presentation of information on relevant Web pages. Web pages should be reviewed and updated as often as necessary. As the use of ICT permeates the FUTO environment, a staff log-in section of the Website will be enabled for staff only information.

6.2 Plagiarism Check

Unless otherwise indicated, this Website and its contents are the property of the Federal University of Technology, Owerri. All articles, thesis or journals to be published should be checked for plagiarism.

6.3 Copyright and Limitation of Liability

The information and materials displayed on the University's website are protected by the relevant Federal laws, International Copyright laws and treaties, and shall not be transmitted, broadcast, copied, adapted, used, distributed or reproduced for commercial purposes without the prior express permission of the Federal University of Technology Owerri.

The Federal University of Technology disclaims liability for any and all claims, losses, costs, expenses (including Attorney's Fees) and damages whatever kind or nature including without limitation, general, special, incidental, consequential, punitive, exemplary damages based on a theory of liability, in connection with any use of the University's web site and the information contained therein.

6.4 Warranties

The University's website may include information from third parties, and links to other websites. The Federal University of Technology Owerri does not make any warranties, expressed or implied, regarding any third-party information or any links to other websites and shall assume no liability or responsibility for the accuracy, completeness, reliability or suitability of the information provided by the third parties.

6.5 Changes

The Federal University of Technology Owerri reserves the right to the terms and conditions or the content of any portion of her website any time without notice.

6.6 Disclaimer

Every subscription, use, access and continued use of the University's website shall be deemed to be subject to the terms and conditions in effect at the point in time.

7.0 THE EDUCATIONAL PORTAL AND OTHER INFORMATION SYSTEMS

- 7.1** The University Educational portal will continue to be used for academic business processes namely; fees payment, course registration, recording of grades, result processing, and lecturer-student interaction forum. The Educational portal shall continue to serve as a repository of academic and allied information or records of students of Federal University of Technology, Owerri, including relevant pre-admission records.
- 7.2** Online Admissions Application System: The Online admissions application systems for prospective undergraduates, postgraduates and allied programmes whereby candidates apply from anywhere in the world, check their results/admission online shall be sustained. These applications shall continue to be accessed from the University Website and be upgraded with advances in technology.
- 7.3** Online Payment System: The fees online payment systems that integrates seamlessly with all major payment gateways in the country (e-Transact, Remita Interswitch, etc.) will continue to be improved so that students can pay fees with their bank ATM credit and debit cards.

8.0 NETWORK DEVELOPMENT AND ICT INFRASTRUCTURE

A Campus Local Area Network (LAN) shall be put in place wired or wireless. Such a network shall be capable of providing staff and students with inter-connectivity on Campus then access to both national and international networks.

With the development of multimedia applications and the increase in computing power on the desk, higher networking speeds and different networking techniques will be deployed as the need arises.

8.1 iPads and Tablets

Laptops, iPads, Tablets and other electronic devices given to university staff because of their position shall remain the property of the University. Such staff will be responsible for the data content of the devices and will return such devices to the University Management if they retire, resign or are redeployed from such positions.

8.2 Computing Facilities and Internet Services

The University shall provide a reliable access to Internet to Departmental ICT Infrastructure; this is in addition to the following:

1. LCD projectors and laptops for lecture rooms.
2. Email services
3. Access to library information resources
4. Computer labs (where mandatory, e.g. Computer Science, Electrical/Electronic Engineering, and Information Management Technology departments etc.)
5. Computers for offices
6. Application software
7. Alternative Power Supply System
8. Other ICT related systems.

8.3 Specialized Computing Requirements

The Computing requirements for systems deployed in various Departments may differ. The fundamental computing requirements for non-data intensive users will be met for all Departmental offices while the specialized computing requirements for data-intensive needs of users in Geosciences, Electrical/Electronic Engineering, Petroleum Engineering, Mechanical, etc. will be taken into consideration.

9.0 POWER SUPPLY AND EQUIPMENT PROTECTION

9.1 Power Supply:

The University shall provide a standby generator for the ICT and Computer Centres in addition to Solar Inverter System for Active Devices, radios, routers, Access Points, wherever they are located on campus.

9.2 Equipment Protection:

The data Centre and Video Conferencing equipment shall have Uninterrupted Power Supply (UPS) and relevant voltage regulator systems to protect the ICT systems from the devastating effects of lighting and larger electrical power switching transient, over-voltages and surges. All buildings with active devices such as access points, towers and antennas should be properly earthed and checked routinely. Telecommunication towers on Campus should be repainted routinely to avoid rust and the integrity should be checked every two years, earthing, aviation lights, stay wires, etc.

10.0 TRAINING AND CAPACITY BUILDING

The University shall give top priority to capacity development of staff of ICT Centre, University Library and Computer Centre. The University shall continue to educate and

sponsor ICT professionals in needed functional areas of their profession to ensure they are up-to-date with emerging Information and Communication Technologies.

A short-term ICT training shall be provided to all relevant University staff to solve identified skill gaps. All staff and students shall be sensitized to acquire basic ICT skills in their own right rather than as adjunct to some other courses.

The University shall create awareness and sensitization to staff, students, parents/Guardians and relevant stakeholders on the application of “Acceptable” and “Non-Acceptable” ICT infrastructure.

11.0 SOFTWARE ACQUISITION AND DEVELOPMENT

The University will endeavor to meet its legal and contractual obligations and will operate effectively and securely in the licensing, purchasing and management of software. The ICT Unit shall ensure that the relevant antivirus/anti-malware is installed on all computers once notified.

11.1 SOFTWARE ACQUISITION

The ICT Centre will be responsible for liaison with the Vice-Chancellor/Registry/all Departments to meet computing resources need and ensure benefit realization from third party application providers. The University ICT Centre shall ensure that no pirated or unlicensed software will be installed on computers or on servers connected to its network.

All the proposed software purchases and acquisitions shall be approved by ICT Centre so that technical, licensing, support, and value for money issues can be adequately considered. The ICT Centre shall maintain an inventory of all University software including the licenses, installations, licensing keys, agreements, media, permitted uses, and the source of funding. It shall also ensure that its use is in accordance with its licensing rules.

The procurement and administration of Unit specific software applications shall be the responsibility of the respective Units. However, the ICT Centre will evaluate all such software to determine its resource requirements, its security capabilities and to make sure that it does not have any legal breaches and there are not already existing University software systems that provide equivalent functions.

11.2 SOFTWARE DEVELOPMENT

The University shall engage in software development projects. These projects shall enable the University to produce application software for industries and also educational software for educational institutions by engaging its staff and students in software development projects.

Any Application Software produced by staff of ICT Centre or Computer Centre using University resources belongs to the University.

12.0 LIBRARY INFORMATION SYSTEM

The University shall provide a library information system to support research, teaching and learning. The integrated on-line library system shall ensure the provision of advanced library computing systems and easy access to library catalogues, databases and ability to share resources among libraries at different locations both locally and internationally.

Additionally, the University Library shall be responsible for the management, acquisition, development and maintenance of the library information system applications, repositories, databases, relevant hardware and software and software needed by the library and its branches.

13.0 HUMAN RESOURCE INFORMATION SYSTEM

The University shall utilize human resource information system as instrument to enhance and streamline human resource management and administrative processes in effective and efficient manner through capturing of personnel information and utilizing it to handle the administrative needs of the Human Resource Management Unit. This will help the University in efficient and accurate planning, recruitment of employees, orientation, training, appraisal, motivation and remuneration.

14.0 E-LEARNING AND SUPPORTING STRUCTRE

The University shall Support and encourage the internal development of the e-learning program by promoting and providing guidelines for training, inclusion of e-learning courses in instructor workloads, and technical support. Also, the use of Learning Management System (LMS) and other technologies in both face-to-face and online learning environments shall be made available for the facilitators and students.

The University shall establish a support unit through the ICT Directorate, to be known as the e-Learning Unit, which will primarily function as a supporting, standard-setting and capacity-building body. The unit shall be responsible in the following areas:

- Promote the use of e-Learning in current and future programmes of the institution.
- Provide training and development for lecturers and facilitators of online learning programmes to ensure effective e-Learning courses and programmes are delivered.
- Set and monitor standards for the use of e-Learning from a technological, content and quality perspective
- Create an enabling environment to promote e-Learning

The ICT Directorate will review the operations of the e-Learning in all the schools in light of the University's e-Learning goals and objectives and work to implement any changes necessary to improve the functioning of the e-Learning effort. The University through the ICT Directorate shall be responsible for promoting the academic integrity of the e-learning courses and also in the training of all academic staff on the e-learning and the use of LMS. The training should be hands-on and regularly updated.

14.1 LEARNER SUPPORT

The University shall ensure that students can be confident that:

- Staff who provide support to learners on these programmes have appropriate skills, and receive appropriate training and development;
- Support for learners, whether delivered through lecturers or through web-based or other distribution channels, meets the expectations of the University for the quality of learner support for a programme of study leading to one of its awards

15.0 IT SUPPORT, BACKUP/RECOVERY AND HELP DESK

15.1 IT Support

The ICT Centre and the University Computer Centre will provide ICT Support to the University Community. The ICT Centre will provide support in the following areas:

- Website, Educational portal and Application Portals
- Provision of FUTO email addresses to staff and students and to withdraw same when necessary.
- Ensure that ICT facilities are functional, operational and well maintained.
- Help Desk Service.
- Back Up/Recovery
- Information Security
- Staff Training
- Maintenance of laptop and desktop computer, printers, plotters and accessories.

The University Computer Centre will provide support in the following areas:

- University and School ICT courses Laboratories
- Staff Training
- Maintenance of laptop and desktop computers, printers, plotters and accessories.

15.2 Backup/Recovery

The purpose of this policy is as follows:

- To provide secure storage for data assets critical to the work flow of official University business.
- To prevent loss of data in the case of accident deletion/corruption of data, system failure, or disaster.
- To permit timely restoration of archived data in the event of a disaster or system failure.

This policy applies to all computers, both mobile and desktop, owned by FUTO.

- Specific locations will be automatically backed up (e.g. My Documents, Desktop, Bookmarks)
- Any location outside of the automated backup locations will be added on a per request basis.

Backups are NOT meant for the following purposes:

- Maintaining a versioned history of data
- Personal data such as photos, videos, music non-business e-mail accounts etc.
- Personal programs (i.e. Applications) of any type.

15.3 Helpdesk Software

The ICT request assists collection of support data. All the tickets are logged into a database. These ticket requests provide valuable information that the University can use to make decisions about improving technical support, purchasing new computers and software applications, upgrading systems and staff training.

16.0 PROCUREMENT AND MAINTENANCE OF ICT INFRASTRUCTURE AND SYSTEMS

The procurement and maintenance of ICT systems requires specialist knowledge and experience, involving technical and contractual issues specific to the ICT market. The risks associated with inadequate control over the procurement and maintenance of ICT equipment (including Hardware: PCs, laptops, servers, external devices, personal digital assistants (PDAs), printers, scanners, routers, switches, radios etc.; Software; Other Services: Cabling, internet hosting, data archiving, etc.) include:

- Incorrect ICT equipment/solutions are acquired
- Inability to provide operational support
- Incompatibility with the University's ICT strategy
- Potential implementation delays
- Contract inefficiencies

It is therefore the Policy of the University that:

- Any ICT procurement should be undertaken by or in proper consultation with the University ICT Directorate, following relevant University procedure in place.
- All ICT procurement should meet the minimum specifications that would be defined by the ICT Directorate from time to time, which should also meet the requirements of the University Contracts Rules, and appropriate authorization must be sought throughout the procurement process.
- ICT Directorate (in consultation with the Directorate of Physical facilities, the Bursary Department and the Legal Unit) has the responsibility for developing specific procurement details.

17.0 DISPOSAL OF OLD COMPUTERS & LIFE CYCLE REPLACEMENT OF COMPUTERS

17.1 Disposal of Old Computers

The University policy for disposal of equipment that is surplus to the requirements of the Unit that originally purchased it is as follows:

- i. Reasonable efforts should be made to see if any other unit is able to make use of the equipment.
- ii. Equipment that has residual value may be sold, either to University members or outside bodies, subject to the University's financial guidelines.
- iii. Where equipment has limited resale value, consideration should be given to whether it can be donated to any charitable or community project.
- iv. If the equipment cannot be reused then it should be recycled or disposed of in an environmentally friendly manner.

17.2 Importance of Data Removal

An overriding consideration in any disposal of equipment must be to ensure that any University data on the machine, and any software licensed to the University is removed. It is, of course, vital to satisfy the requirements of the Data Protection Act, but it must also be understood that any University data that is discovered by a later owner may cause controversy, adverse publicity etc.

Ensuring adequate destruction of data is the responsibility of the Unit that owns the equipment, and must not be delegated to any person outside the University-without adequate contractual obligations being imposed.

Before disposing of any computer system, it is vital to remove all traces of data files. Merely deleting the visible files is not sufficient to achieve this, since data recovery software could be used by a new owner to "undelete" such files. The disk-space

previously used by deleted files needs to be overwritten with new, meaningless data- either some fixed pattern (e.g. binary zeroes) or random data. Similarly, reformatting the whole hard disk may not in itself prevent the recovery of old data as it is possible for disks to be “unformatted”. Profession tools for wiping data should be used or reformatting the hard disk and reinstalling a new operating system can be used to ensure deletion of data.

18.0 ACCEPTABLE USE

The University 's ICT facilities are provided to support teaching, learning, research and administrative activities or any purpose that is in accordance with the aims and policies of the University.

Every staff is responsible for activities conducted using his/her user account. The following outlines Acceptable use of FUTO ICT facilities.

- a. Only staff and registered students of the University or those authorized by the designated authority are permitted to use the University's ICT facilities.
- b. An electronic mail (email) system will be one official mode of information dissemination to the University community. Information such as memos, notices, administrative communication, and bursary information can be disseminated using the FUTO email account.
- c. Staff should not access the educational portal from Public Cybercafé.
- d. The University ICT facilities and service must not be used for any unlawful purpose.
- e. The University reserves the right to monitor, log, collect and analyze the activities of users in their usage of ICT facilities and services.
- f. The ICT facilities include but not limited to University owned or leased desktops. Laptops, mobile devices, email, telecommunication systems, LAN, wireless network.
- g. Users should not expect privacy while using University owned or leased equipment.
- h. The University reserves the right to block or filter any network traffic that potentially breaches the ICT policy of is potentially illegal since inappropriate use exposes FUTO to risks including attacks from malicious software, disruption, compromise of ICT systems and services and legal issues.
- i. Staff and students are expected to check and respond to emails regularly, at least once daily for staff and one every other day (48 hours) for students.
- j. Staff and students shall make reasonable effort to ensure that they send data that is Virus Free and to protect themselves from viruses and hacking attempts when connected to the University's network.
- k. Staff and students are to be prepared to show their ID cards as proof of identity, whenever, they are required to do so at the University ICT Centre, University Computer Centre and the University Library.
- l. Staff and students are to safeguard their passwords and access identities to all University systems.

- m. Staff and students shall inform Help Desk of any communication, system problem, or other circumstance that may indicate a breach of security or other risk to the integrity of the ICT system.
- n. Staff and students shall immediately request a new password and ID, when they report if one's password and ID has become compromised.
- o. Staff and students must not leave one's computer unattended while connected to the Internet.
- p. Staff and students must not enable any program or macro/agent to automatically forward Intranet mail to or via the Internet or any other external system.

The ICT Centre shall ensure the following:

- i. All outbound Internet traffic from the University's network zone should pass through a web filtering gateway.
- ii. Access to sites categorized as being potentially harmful to the Centre will be blocked.
- iii. All Internet traffic (inbound and outbound) should pass through an antivirus gateway.
- iv. At a minimum, up-to-date anti-virus and anti-malware software should be installed and running on workstations with Internet connectivity.
- v. A log should be created that records all requests (both inbound and outbound) for Internet services. The generated audit logs should be reviewed on a monthly basis by the designated ICT staff of the Centre.

19.0 UNACCEPTABLE USE

The Internet provides access to an array of information, resources and services that aid and support the work of the staff and students. However, if Internet use within the University Network is not securely managed, it can expose the University to risks at both a technical level with potential damage being caused to ICT infrastructure and possible reputational damage.

Unacceptable use of University ICT facilities may be summarized as follows:

- a. The FUTO email account must not be used for sending religious, social or non-official emails, spam, photos etc.
- b. Allowing the University's ICT facilities to be damaged or contaminated by food, drink or other materials.
- c. Deliberate or unauthorized access to the University's networked facilities or services.
- d. Revealing your account password to others or allowing use of your account by others.
- e. creation or transmission or causing the transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into

- obscene or indecent images or material (posting of defamatory comments about staff or students on social networking sites.)
- f. Using the University's ICT facilities to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
 - g. Accessing, creating, changing, storing, downloading, or transmitting material which may be deemed offensive, threatening, abusive, discriminatory or otherwise to cause annoyance or inconveniences.
 - h. Interfering with the legitimate use by others, or interfere with or remove computer printout or media belonging to others.
 - i. Violating the privacy and confidentiality of anyone else, such as sending unsolicited email messages or other digital information or falsify emails/information to make them appear to have been originated from someone else.
 - j. Introduction of malicious programs into the University's network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).
 - k. Unauthorized copying of copyrighted material including but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music.
 - l. Installation of any copyrighted software for which the University or the user does not have an active license (Installation of unlicensed or illegal software on university systems).
 - m. Using University's ICT facilities for commercial, social or group distribution activities unless permission has been formally granted.
 - n. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable, a user's access and use of the ICT facilities (Unsolicited advertising, often referred to as spamming).
 - o. Using University facilities and or services in order to gain privileges which have not been authorized.
 - p. Streaming non-academic related audio or video.
 - q. Downloading, uploading, distribution, or storage of music, video, film or other material, for which you do not have valid permission from the copyright holder;
 - r. Deliberate viewing, downloading or printing of pornographic images.
 - s. Must not enable any program or macro/agent to automatically forward Intranet mail to or via the Internet or any other external system.
 - t. It is a violation of this policy to use the University's ICT facilities for any activity that is illegal under state, Federal or International law. Such activities include but not limited to posting fake information on social, media, spoofing, phishing, ping attack etc.

19.1 Infringement

The University reserves the right to treat any infringement or infraction of the Acceptable and unacceptable use of ICT facilities as summarized in paragraph(s) **17.0-18.0** above, as Minor, Major or Gross Misconduct in the context of the

University Regulations, depending on the gravity and shall impose appropriate disciplinary measures as prescribed in the University Act and Regulations for each category of the Misconduct, in event of proven cases of infraction as the case may be.

20.0 POLICY IMPLEMENTATION & RESPONSIBILITY

FUTO ICT Policy shall be made effective by the relentless effort of the ICT Directorate under the Vice-Chancellor's directive. Both staff and students will be provided a reasonable level of privacy and confidentiality, the data they create on the corporate systems remains the property of the University.

The University reserves the right to withdraw access to ICT facilities from any user(s) that have not complied with this policy.

The University Network and systems will be audited on a periodic basis to ensure compliance with the Policy. Users found to have violated the policy standards shall be guilty of misconduct which shall be addressed by established University and National legal processes. In case of violation, the ICT Directorate will be consulted to provide oversight, insight and guidance with respect to where they are required and applied. The Implementation and Responsibility of each policy issue is summarized in the following table:

TABEL 1: POLICY IMPLEMENTATION AND RESPONSIBILITES

S/N	POLICY	ENFORCEABLE BY	ACTIONS/PENALTY/SANCTIONS
1.	University Website	ICT Directorate and IPPA	a. ICT Directorate should be alerted and appropriate disciplinary action should be taken against the user(s) for total misconduct following due process. b. IPPA shall be responsible for news and information.
2.	Unit's Website Pages	Deans, Heads of Depts./Units	Deans will be responsible for School Web pages while Heads of Departments, Units will be responsible for their Departments, Units pages.
3.	Plagiarism Check	University Administration	Management to take appropriate disciplinary action following due process.
4.	Educational portal	ICT Directorate	ICT Directorate should be alerted and appropriate disciplinary action should be taken against the use(s) for total misconduct following due process.

5.	Network Connectivity	ICT Directorate	ICT Directorate should be alerted and appropriate disciplinary action should be taken against the user(s) for total misconduct following due process.
6.	Departmental Infrastructure	ICT Directorate/University Administration/Schools	ICT Directorate to advice Management to take correct measure for defaulter(s).
7.	Social Media Posts	ICT Directorate	University Management to take appropriate action.

21.0 ABBREVIATIONS

S/NO	ABBREVIATION	FULL MEANING
1.	ICT	Information and Communication Technology
2.	IP	Internet Protocol
3.	LAN	Local Area Network
4.	CAD	Computer Aided Design
5.	CBT	Computer Based Training
6.	CCE	Centre for Continuing Education
7.	DBMS	Database Management System
8.	DNS	Domain Name Service
9.	EMAIL	Electronic Mail
10.	FTP	File Transfer Protocol
11.	LIBIS	Library Information System
12.	TCP	Transmission Control Protocol
13.	URL	Universal Resource Locator
14.	WAN	Wide Area Network
15.	WWW	World Wide Web
16.	VSAT	Very Small Aperture Terminal
17.	VOIP	Voice Over Internet Protocol

22.0 DEFINITION OF TERMS

S/NO	TERMS	DEFINITIONS
1.	ICT	Use of any equipment which allows users to communicate or manipulate information electronically
2.	Users	FUTO community members who use ICT resource to their own advantage such as staff, students. ³
3.	Spam	Illegal and/or unrequested electronic mass mailings
4.	Port Scanning	Constant querying of a computer or network device
5.	Network Sniffing	Tracing and recording of data travelling between computers on the network by attacking a device or a program to a network
6.	Spoofing	Planned persuasion of influence of user or a computer device to carry out wrong activities by copying or holding as a legitimate source.

7.	Ping Attack	An attack process where a computer in a network gets “pinged” which means it receives echo-request from another computer in a continuous rate, hence preventing the computer from having contact with another.
8.	Password	Strings of characters required in conjunction with the “username” unlock the computer to gain access to some resources. It provides high level of security.
9.	Stakeholder	Any person, department, unit or organization that has interest in an information and communication Technology.
10.	ICT Project	Any ICT contract or work that happens only with defined starting and stopping time with a view to create or implement a specific ICT Technology, Product, Knowledge or Service.
11.	Hardware	Such as scanners, printers, cameras, CD-ROMs (Read Only Memory, Compact discs), network cards, multimedia equipment, UPS, fax machines and one used in the network.
12.	Browser	Software package that allows the user to find view, upload and download information over the Internet.
13.	Uniform Resource Locator (URL)	Internet Address that shows which area of the Internet will be accessed.
14.	World Wide Web	All the resources and users on the Internet that make use of the Hypertext Transfer protocol (HTTP).
15.	Privacy	The right to be left alone or to be withdrawn from public view prevent illegal collection and use or misuse of data.
16.	Peripheral	Physical components of the computer including printers, scanners, cameras, UPS, fax machines etc. That are used in the network.
17.	Computer	Device that accepts data, processes it and generates information with the help of stored program.
18.	Network	Linked computers in order to share resources.
19.	Internet	Gigantic network of networks globally accessed.
20.	Email	Sending and receiving of electronic messages, documents and files in data, text, voice or multimedia form over computer network.
21.	Emails Bombs	Deceitful mails received as a result of sending large volume of email to an address in an attempt to flood the mail box.
22.	Hacking	Unauthorized access and use of networked computer system with a view to steal or damage data and programs.
23.	Packet	A unit of information that is transferred in all computers in a network.
24.	IT Backup	Copying out files or database so that they will be secured in case of equipment failure or other destructions (catastrophe)
25.	ICT Security	Responsible for ensuring that information & information systems such as intellectual properties, cooperate applications

		and student's records are safe, secured and protected.
26.	Computer virus	A program code that cannot work without being inserted into another program.
27.	Computer worm	A distinct program that can run independently. Both virus and worm copy destructive routines into the networked system which affects any computer that uses copies of magnetic disks taken from infected computers.
28.	Phishing	Attempts to obtain sensitive information such as a Username, password and credit card details from an unsuspecting victim by masquerading as a trustworthy entity.

23.0 DOCUMENT SCOPE, CONTROL AND REVISION

This policy applies to all staff, students and all relevant stakeholders within the University. The ICT Centre will maintain control of the Policy document as directed by University Management. Meticulous re-visitation and review of the Policy is recommended within a space of two (2) years.

Adequate monitoring and review process must be established to achieve effective ICT services.

Prof. (Mrs) Nnennaya N. Oti
Vice-Chancellor