Information and Communication Technology (ICT) Policy

Table of Contents

1. Introduction

Information and Communication Technology (ICT)[1] has brought in fundamental changes in all aspects of our society today. It is clear that effective and efficient operation of core University business (Teaching, Learning, Research and Administration) depend heavily on ICT. It is based on the potential role of ICT in education that the University management has committed and invested so much on it. In order to ensure that the University's ICT facilities are well utilized, managed and protected, Management constituted committee to develop an ICT Policy (a wide range of regulations and guidelines with respect to the use, maintenance, and security of the University's ICT facilities).

This document defines the University of Jos Information and Communication Technology (ICT) Policy. The policy applies to to all Users[2] at the University of Jos' ICT facilities, which include but are not limited to the following:

1. Network infrastructure, including the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers
2. Network and Internet services, including internet access, web services, email, wireless, messaging, telephony and fax services
3. Computing hardware, both fixed and portable, including personal computers, workstations, laptops, personal digital assistants (PDAs), servers, printers, scanners, disc drives, monitors, keyboards, tablets and pointing devices
4. Software and databases, including applications and information systems, content management systems, learning management systems, websites, email systems, etc.
5. Development training programmes to provide staff and students with basic ICT skills.

The policy is subdivided into:

- General – University Responsibility
- Procurement and Maintenance of ICT Infrastructure and Systems
- Acceptable and Unacceptable Use
- Security, Privacy and monitoring

This policy document sets out the University's aims, principles and strategies for the delivery of Information and Communication Technology. It will form the basis for the development of ICT in the University.

[1] The term Information Communication Technology (ICT) is here defined as the use of any equipment which allows users to communicate or manipulate information electronically.

[2] The term Users refers to: University staff, students, consultants, visitors, contractors, authorized guests and other personnel

2. The Policy

2.1 General – University Responsibility

It is the responsibility of the University:

1. to provide a working environment that encourages access to knowledge and sharing of information through ICT
2. to put in place ICT facilities for staff and students to access information through:
    a. Faculty/Departmental/Unit Computer Labs
    b. Network points in all offices and laboratories
    c. Provision of computers in staff offices and laboratories
    d. Provide dedicated band width for academic purposes
    e. Provision of ICT facilities in students accommodation
3. to take responsibility for issuing University of Jos email addresses to staff and students and to withdraw same when necessary
4. to provide basic ICT skills to staff and students through Development Training Programs
5. to ensure secured access of individual data and information. The university shall not be liable for any damage to users' system or information that occurs through virus or hacking attacks
6. to ensure that ICT facilities are functional, operational and well maintained
7. to setup appropriate mechanisms for digitization of University's historical data and information (including students records, university achieves, inventory systems, bursary, human resource (HR) Information)
8. to provide a reasonable level of privacy and confidentiality, but staff and students should be aware that the data they create on the corporate systems remains the property of the University
9. to reserve the right to withdraw access to ICT facilities from any user(s) that have not complied with this policy
10. to reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.2 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[3] includes:

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

[3] ICT Facilities include: 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

- Etc

It is therefore the Policy of the University:

1. that any ICT procurement should be undertaken by, or in proper consultation with the University ICT Directorate, following relevant University procedure in place
2. 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 correct authorisation must be sought throughout the procurement process
3. that maintenance and support of all ICT facilities is also to be carried out by the University's ICT directorate. For maintenance and support, all networked servers are to be situated at the University's main data centre.
4. that procurement and maintenance of internet connectivity is to be provided to the University community through the ICT directorate
5. that ICT directorate (in consultation with the Directorate of Physical facilities, the Bursary and the Legal unit) has the responsibility for developing specific procurement details.

2.3 Acceptable and Unacceptable use

The acceptable and unacceptable use policy aims at defining what staff and students can and cannot use the University's ICT facilities for.

2.3.1 Acceptable Use

It is the policy of the University:

1. that 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
2. that staff and students can use the facilities for official activities as defined in 1 above
3. that only staff and registered students of the University or those authorised by the designated authority are permitted to use the University's ICT facilities
4. that 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 will be disseminated via email. The University website will also be used for disseminating information to the University community.
5. that staff and students are expected to:
    a. check and respond to emails regularly, at least once daily for staff and once every other day (48 hours) for students
    b. respect the rights of others, and conduct themselves in a quiet and orderly manner when using open access ICT facilities
    c. 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
    d. respect the published times of access to open ICT facilities
    e. be prepared to show their ID cards as proof of identity, whenever required to do so

f. safeguard their passwords and access identities to all University systems
g. comply with the bandwidth, data storage and other limitations on services
h. conform to all other appropriate policies and guidelines from the ICT directorate and the University

6. that because of the need to protect the University's network, the University shall not be liable for any breach of confidentiality of information stored on any network device belonging to the University .

2.3.2 Unacceptable Use

Use of the University's ICT facilities for any activity that is illegal under state, federal or international law while utilizing the University's ICT facilities violates this policy. It is the policy of the University to prohibit the use of its ICT facilities for the activities though not restricted to the underlisted:

1. using ICT Facilities shall not be prejudicial to the interest and good name of the University
2. allowing the University's ICT facilities to be damaged or contaminated by food, drink or other materials
3. deliberate or unauthorised access to the University's networked facilities or services
4. revealing your account password to others or allowing use of your account by others
5. 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
6. 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
7. accessing, creating, changing, storing, downloading, or transmitting material which may be deemed offensive, threatening, abusive, discriminatory or otherwise to cause annoyance or inconveniences
8. interfering with the legitimate use by others, or interfere with or remove computer printout or media belonging to others
9. 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.
10. introduction of malicious programs into the University's network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
11. unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music
12. installation of any copyrighted software for which the University or the user does not have an active license
13. using University's ICT facilities for commercial, social or group distribution activities unless permission has been formally granted

14. 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
15. using University facilities and or services in order to gain privileges which have not been authorised
16. reselling, sharing or otherwise distribution of services or any portion thereof to any third party.

2.4 Security, Privacy and Monitoring

This policy sets out the University's approach to monitoring users responsibilities with respect to security and privacy. It is the policy of the University that:

1. users are responsible for any misuse of the ICT facilities and or services that originate from their account, even for activities committed by a friend, family member or co-worker, co-student, or anyone having access using your account details
2. users are responsible for the security of any device/computer they use to connect to the University network or Internet services
3. facilities or and services shall not be used to breach the security of another user or to attempt access to anyone's computer, data or services without the knowledge and consent of that person
4. monitoring network traffic at the University will involve only the collection of packet header information, not the packet data, unless required to check for viruses, to monitor the improper release of confidential information. Note that executing any form of network monitoring tools must be done by Directorate
5. the University Chief Security Officer will be the contact point for investigating reported cases of indecent, unauthorized or suspicious activities
6. the ICT directorate will monitor the University's Network Backbone 24 hours, 7 days a week. All network failures and excessive utilization will be reported to the technical staff for problem resolution or design enhancement.
7. the ICT maintenance and Support Service Unit will act as the Point of Contact for network and computer related problems
8. all security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    a. all security related logs will be kept online for a minimum of 1 week.
    b. daily incremental tape backups will be retained for at least 1 month.
    c. weekly full tape backups of logs will be retained for at least 1 month.
    d. monthly full backups will be retained for a minimum of 2 years.
9. the University's ICT directorate is authorized to routinely monitor traffic on the network backbone (only nominee of the Director). Personnel authorized to analyze network backbone will not disclose any information obtained in the process without approval of the Dean or Heads of Departments/units
10. measures for effective security breaches or disruptions of network communication would be in place. For purposes of this section, "disruption" includes, but is not limited to,
    a. network sniffing
    b. pinged floods
    c. packet spoofing
    d. denial of service
    e. forged routing information for malicious purposes

11. staff and students should be aware that logs are generated by the various Internet services used, including email, web access and network flows. While it is not the policy of the University to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the University's Internet links. Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.
12. provision of data and information relating to the University's staff and students to parties outside the University must be approved by the University Management
13. all devices connected to the University's network must be centrally registered with the Directorate

3. Policy Enforcement

Users found to have violated this policy shall be guilty of misconduct in accordance with the University Act and the Rules and Regulations governing the conduct of the University's business.

4. Policy Implementation and Responsibility

Implementation and responsibility of each policy issue is summarized in the following table:

POLICY	IMPLEMENTATION STATUS	ENFORCEABLE BY	PENALTY/SANCTIONS
General			
2.1.1	In progress	University Administration	Not Applicable
2.1.2(a) 2.1.2(b) 2.1.2(c) 2.1.2(d) 2.1.2(e)	In progress	University Administration	Not Applicable
2.1.3	Already in place	University Administration	Not Applicable
2.1.4	In progress	University Administration/ Staff Training Development Office	Not Applicable
2.1.5	In progress	ICT Directorate	Attention of the Directorate should be drawn and an appropriate disciplinary action should be taken against the officer(s) for gross misconduct following due process.
2.1.6	Partially in place	ICT Directorate	Attention of the Directorate should be drawn and an appropriate disciplinary action should be taken against the officer(s) for gross misconduct.

2.1.7	Just taken off	University Administration, ICT Directorate	Directorate to be responsible and appropriate disciplinary action should be taken against the officer(s) for gross misconduct.
2.1.8	In place	ICT Directorate	Attention of the Directorate should be drawn and an appropriate disciplinary action should be taken against the officer(s) for gross misconduct.
2.1.9	Not in place	University Administration ICT Directorate	Access to facilities denied. Cases of violation to be reported to management for appropriate disciplinary action.
2.1.10	Not in place	ICT Directorate	Directorate to report cases of policy violation to management for appropriate disciplinary action.
Procurement and Maintenance of ICT Infrastructure and Systems			
2.2.1	Partially in place	ICT Directorate/ University Administration	Directorate to advice Management to take appropriate measure for non-compliance.
2.2.2	In place	ICT Directorate/ University Administration/ Faculties/ Depts/ Units/ Contractors	Directorate to advice Management to take appropriate measure for non-compliance.
2.2.3	Partially in place	ICT Directorate/ University Administration	Directorate to advice Management to take appropriate measure for non-compliance.
2.2.4	Already in place	ICT Directorate	Attention of the Directorate to be drawn and an appropriate disciplinary action to be taken against violation.
2.2.5	Not in place	ICT Directorate	Directorate to advice Management to take appropriate disciplinary action to be taken against violation.
Acceptable and Unacceptable Use			
Acceptable Use			
2.3.1.1	In progress	University Administration/ICT Directorate	Directorate to report cases of violation to Management for an appropriate disciplinary action on the violator following due process.
2.3.1.2	In progress	University Administration/ ICT Directorate	Directorate to report cases of violation to Management for an appropriate disciplinary action on the violator following due process.
2.3.1.3	Not in place	University Administration/ ICT Directorate/Fac./ Depts./Units	Directorate to report cases of violation to Management for an appropriate disciplinary action on the violator following due process.
2.3.1.4	Partially in place	University Administration/ ICT Directorate	To be enforced
2.3.5.1(a)	Not in place	University	Management to take appropriate

		Admin/ICT Directorate/Staff/Students	disciplinary action following due process. For students, University Administration will not be liable.
2.3.5.1(b)	To be implemented	University Admin/ICT Directorate/Fac/ Dept/Units	ICT Directorate to report cases violation to Management for appropriate disciplinary action following due process.
2.3.5.1(c)	Partially in place	ICT Directorate	ICT Directorate to report cases of violation to Management for appropriate disciplinary action following due process.
2.3.5.1(d)	Partially in place	ICT Directorate/Fac/ Depts/Units – ICT Coordinators	ICT Directorate to report violation to Admin for appropriate disciplinary action following due process.
2.3.5.1(e)	Partially in place	ICT Directorate/Fac/ Depts/Units – ICT Coordinators	Access to facilities denied. Cases of violation to be reported to the Security for appropriate sanction.
2.3.5.1(f)	Partially in place to be enforced	ICT Directorate/Staff/ Students	University shall not be liable for any loss of personal data or information. However, the violator shall be liable for any damage to University facilities.
2.3.5.1(g)	Partially in place	ICT Directorate	ICT Directorate to report any violation to the University Administration for necessary disciplinary action.
2.3.5.1(h)	Partially in place	University Adm./ICT Directorate	ICT Directorate to report any violation to the University Administration for necessary disciplinary action.
2.3.1.6	Not yet in place	University Administration/ ICT Directorate	ICT Directorate to report any violation to University Administration for disciplinary action following due process.
Unacceptable Use			
2.3.2.1	Not yet in place	University Administration/ ICT Directorate	ICT Directorate to report cases of violation to Management for disciplinary action following due process.
2.3.2.2	Partially in place	University Administration/ ICT Directorate/Fac/ Depts/Units	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.3	Not yet in place	University Administration/ ICT Directorate	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.4	Not yet in place	University Administration/ ICT Directorate/ Staff/ Students	Users are liable to any violation and Management to take any appropriate disciplinary action once reported by the ICT Directorate.

2.3.2.5	Not yet in place	University Administration/ ICT Directorate/Fac/ Depts/Units	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.6	Not yet in place	University Administration/ ICT Directorate/Fac/ Depts/Units	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.7	Not yet in place	University Administration/ ICT Directorate/Fac/ Depts/Units	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.8	Not yet in place	University Administration/ ICT Directorate/ Staff/ Students	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.9	Not yet in place	University Administration/ ICT Directorate	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.10	Not yet in place	University Administration/ ICT Directorate	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.11	Not yet in place	University Administration/ ICT Directorate/Fac/ Depts/Units	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.12	Partially in place to be enforced	University Administration/ ICT Directorate/	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.13	Not yet in place	University Administration/ ICT Directorate/Fac/ Depts/Units	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.14	Not yet in place	University Administration/ ICT Directorate/ Staff/ Students	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.15	Not yet in place	University Administration/ICT Directorate/Fac/ Depts/Units	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.3.2.16	Not yet in place	University Administration/ICT Directorate	ICT Directorate to report any violation to Management for disciplinary action following due process.
Security, Privacy and Monitoring			
2.4.1	Not yet in place	University Administration/ICT Directorate	ICT Directorate to report any violation to Management for disciplinary action following due process.
2.4.2	Not yet in place	ICT Director	Violators to be denied access to

			facilities. In cases of violation, Users to be reported to Management for disciplinary action following due process.
2.4.3	Not yet in place	University Administration/ICT Director	Violation to be reported to Management for disciplinary action following due process.
2.4.4	Partially in place	ICT Director	ICT Directorate to report to Management for appropriate disciplinary action following due process.
2.4.5	Not yet in place	ICT Director/Fac/ Depts/Units	Chief Security Officer reports to Management for disciplinary action.
2.4.6	Partially in place	University Administration/ ICT Director	Not Applicable
2.4.7	Not yet in place	ICT Directorate/Fac/ Depts/Units/Staff/Students	ICT Director report to the Management for appropriate disciplinary action following due process.
2.4.8(a) 2.4.8(b) 2.4.8(c) 2.4.8(d)	Partially in place	University Administration/ ICT Directorate	ICT Director report violators to Management for appropriate disciplinary action.
2.4.9	Partially in place	ICT Directorate	ICT Director report violators to Management for appropriate disciplinary action.
2.4.10(a) 2.4.10(b) 2.4.10(c) 2.4.10(d) 2.4.10(e)	Not yet in place	ICT Directorate	ICT Director report violators to Management for appropriate disciplinary.
2.4.11	Not yet in place	ICT Directorate	ICT Director report violators to Management for appropriate disciplinary action.
2.4.12	Partially in place	University Administration	Not applicable
2.4.13	Partially in place	ICT Directorate	ICT Director report violators to Management for appropriate disciplinary action.

University of Jos Policy Implementation Table

7. Other References

Users are bound by the law of the Federal Republic of Nigeria when using the University's ICT facilities and services. In addition, when accessing computers and or services abroad the rules and law of that country apply.

Note that it is the responsibility of every user to ensure that their activities comply with these laws.

Definition of Terms

S/No	Terms	Definitions
1	ICT	Information and Communication Technology
2	Peripheral	an ICT equipment that can be attached to a computer to be operated under a computer control (e.g. Printers, USB memory, digital cameras, etc)
3	Computer	any device that manipulates data according to a list of instructions
4	Network	Interconnected computers
5	Internet	an internetwork consisting of a worldwide interconnection of governmental, academic, public, and private networks.
6	SPAM	unauthorised and /or unsolicited electronic mass mailings
7	Email bombs	a form of abuse caused as a result of sending huge volumes of email to an address in an attempt to overflow the mailbox *or* overwhelm the server
8	Hacking	an attempt to defeat or exploit the security capabilities of a computer or network
9	Obscene or indicant images	Images that are deemed deeply offensive according to contemporary community standards of morality and decency.
10	Password	a word or string of characters that is entered, often along with a 'username', into a computer system to login or to gain access to some resource. Passwords are a common form of authentication
11	Privacy	ability of an individual or group to seclude themselves or information about themselves, but could chose to reveal themselves selectively
12	Confidentiality	ability to ensure that information is accessible only to those authorized to have access
13	Packet	a unit of information transport in all computer networks
14	Packet header information	the portion of an Internet Protocol (IP) packet that precedes its body and contains addressing and other data that is required for it to reach its intended destination
15	Packet data	also referred to as 'packet body' is the actual data that the packet is delivering to the destination.
16	Virus	a small computer program that is designed to spread from one computer to another and to interfere with computer operation without permission or knowledge of the user that. A virus might corrupt or delete data on your computer, use your e-mail program to spread itself to other computers, or even erase everything on your hard disk. Viruses are mostly and easily spread by attachments in e-mail messages or instant messaging messages. That is why it is essential that you never open e-mail attachments unless you know who it's from and you are expecting it.

17	Worms	a is a self-replicating computer. It uses a network to send copies of itself to other computers and devices on the network and it may do so without any user intervention.
18	Trojan horses	also known as a 'Trojan' is is malware (a computer program) that appears to perform a desirable function but in fact performs undisclosed malicious functions.
19	Sniffing	An act widely used by hackers and crackers to gather information (capturing packets of data flowing across a computer network) illegally about networks they intend to break into Note that sniffing has legitimate uses to monitor network performance or troubleshoot problems with network communications.
20	Ping floods	a simple DoS attack where the attacker overwhelms the victim with ping packets.
21	spoofing	an act of creating IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.
22	Denial of Service attacks	DoS attacks for short are an attempt to make a computer or network resource unavailable to its intended users.
24	Electronic log	a record of important events