# ICT POLICIES

## REGULATIONS GUIDING INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) OPERATIONS

## IN

## BENUE STATE UNIVERSITY, MAKURDI

# 1.0 INTRODUCTION

[

ICT (Information Communication Technology) refers to technology that is used for processing and distribution of data/information using computer hardware and software, telecommunications, and digital electronics. ICT has become an enablement tool for any activity and business process of an organization. This ICT policy document articulates policy guidelines and framework as program of actions adopted by the University ICT Policy and Management Committee for the development and application of ICT by all units of the University that will support teaching and learning. This will be achieved by integrating ICT into teaching, learning, research, information dissemination and management activities to close the knowledge and technology gap that hitherto exist within the system and place global information grid at the disposal of University community, it also contains punitive measures against non-compliance aimed at protecting the rights of staff and students and other stake holders of the University.

# 2.0 PURPOSE AND SCOPE

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

## 2.1 PURPOSE

The purpose of this ICT document is to:

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

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

iii. Ensure that ICT resources are used efficiently and appropriately in support of teaching, learning, research and administrative functions of the University.

iv. Encourage and create awareness so as to enable users to understand their own responsibility for protecting ICT resources.

v. Ensure that resources are secured and protected against abuse, damage, loss or theft.

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

vii. Provide mechanisms for taking/hearing of external and internal complaints about actual or perceived abuses against the university ICT systems.

viii. Reduce interruptions and ensure a high availability of an efficient network essential for sustaining the business of the university.

ix. Ensure compliance without limitation to statutes and regulatory frame works.

## 2.2 SCOPE

This document provides the policy framework for:

i. Promoting e-learning
ii. Development and use of Management Information Systems (MIS)
iii. Managing ICT services and Network infrastructures
iv. Secure and acceptable use of ICT facilities
v. Use of internet services and Applications
vi. Information and Communication Technology (ICT) procurements and
vii. ICT Project Management.

The ICT facilities covered under this policy document include;

i. BSU network infrastructure; this includes (but not exclusively) the physical infrastructure such cables, wireless devices, network servers, firewall/defenses, connections, switches and routers.
ii. BSU network services; this includes (but not exclusively) internet access, intranet, web services, email, wireless, messaging, shared file stores, printing, telephony and fax services, CCTV, door and car park access control.
iii. BSU owned computer hard and accessories; this include university owned or leased computing hardware both fixed and portable including (but not exclusively) personal computers, workstations, laptops, tablets, PDA's, mobile devices, smart phones, serves, printers, scanners, disc drives, monitors, keyboards and pointing devices.
iv. BSU owned ICT related electronic devices; this includes (but not exclusively) touch screen boards, computer projectors, projector screen, video and digital cameras.
v. BSU software and database; this covers applications and information systems, virtual learning and video conferencing environments, ICT laboratories, software tools, information services, electronic journals and e-Books.

## 3.0 POLICY STATEMENT

Any individual using the ICT facilities in Benue State University, Makurdi is deemed to have accepted this Policy and is bound by it.

ICT facilities are provided to Users primarily for University business purposes to support teaching, learning, research, professional, and administrative activities, in addition occasional and limited personal use of the facilities by staff and students is allowed. The University's business purposes (primary purpose) of ICT facilities take priority over personal use. Email accounts are created for all Staff to foster stronger communication links between Staff and Students.

Any infringement of these regulations may be subject to penalties under civil or criminal law, and such law may be invoked by the University. Any infringement of these regulations constitutes a disciplinary offence under the University's procedures and may be treated as such regardless of legal proceedings.

These policies do not form part of the contract of employment and can be amended without users consent, the university may therefore make changes to the policy at any time and users will be notified of any changes.

## 4.1 ACCESS MANAGEMENT AND CONTROL

To prevent or minimize unauthorized access to computer systems or damage, theft or loss of equipment, the following shall be enforced:

4.1.1 Physical Access Control

i. The Directorate of ICT shall ensure access control to server rooms, computer labs and other major ICT facilities. They should be adequately secured at the doors and windows and only authorized staff shall be granted access.

ii. All ICT equipment must be labeled appropriately for identification

iii. The Directorate of ICT shall put signs or sign boards labeled as "Only Authorized Person is Allowed" at entrance of secured areas.

iv. All units shall be required to maintain an Asset Register to record and track their computer equipment. In addition the Directorate of ICT shall maintain a centralized Asset Register to track the computer equipment in the University.

v. During non-working hours, secured areas shall be protected against physical intrusion by appropriate access control, locks, and surveillance systems or by security staff.

4.1.2 Safety Rules

i. The Directorate of ICT has to set out procedures that will prevent anticipated threats that may damage physical devices.

ii. All devices shall be installed by authorized ICT staff only after consulting the installation guide and manual of the respective device. Failures that arise from violating this section will result in Administrative penalty.

iii. Directorate of ICT shall take appropriate precaution to protect electric devices from power surge and data loss that may occur as result of electrical power interruption and fluctuations by the installing uninterrupted power supply (UPS) and surge protection devices wherever practical.

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

vi. All ICT resource and infrastructure shall be ergonomically correct and shall not entail physical or physiological impact or damage for user.

### 4.1.3 Logical Control and Access to the Internet:

Access to the University network facilities (Local Area Network) shall be controlled through the following:

i. Access to the Internet shall be through User IDs and Passwords using authorized computer hardware. All users (staff and students) should obtain their passwords at the ICT helpdesk.
ii. All data packets and connection requests will be controlled by a central firewall and only explicitly permitted traffic is allowed through the firewall.
iii. All traffic passing through the firewall must be capable of being logged and audited.

### 4.1.4 Network Control:

i. Clearance should be sought from the Directorate of ICT for any third-party network connections to the Internet or any external networks.

ii. Computers, workstations and laptops, PDA and smart phones or other removable storage devices such as USB drives or memory sticks may be connected to University network subject to the approval of the Directorate of ICT.

iii. The Directorate of ICT shall secure the University network infrastructure from email spam, intruder or hackers, virus, worms and other disruptive software.

### 4.1.5 User Responsibilities

i. Users must take all reasonable steps to ensure that computer equipment in their possession or under their control are protected at all times against theft, accidental or deliberate damage.

ii. Users should take reasonable care to safeguard the ICT equipment.

iii. Only university's staff and students are allowed to use the university's ICT facilities. Visitors and quests shall obtain authorization from the User Support Unit.

4.1.6 Antivirus

i. The Directorate of ICT will ensure all computers and other devices connected to the network must have the University's standard antivirus software installed.

ii. For computers not connected to the network, the officer in charge at the Department should liaise with the Directorate of ICT to have updates done regularly.

iii. Any software or data received from any external source, including the original manufacturer and the internet, must be treated as suspect and not installed, executed or used in any other fashion until it has been scanned for viruses using the University's standard virus detection software.

iv. Users should call the attention of ICT helpdesk if a virus incident or activity is noticed and cannot be cleaned by the user.

4.1.7 Third Party Access

i. Entities other than the Directorate of ICT may neither negotiate nor grant third parties access to the University's applications, databases, communications and network infrastructure.

ii. Applications for access should be made in writing to the Director of ICT.

## 5.1 POLICY ON REPAIRS, DISPOSAL AND DISASTER RECOVERY

5.1.1 Troubleshooting, Repairs, Maintenance and Disposal

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

ii. User Departments may contract an external ICT service company to repair and maintain their computer equipment under the supervision of the Directorate of ICT.

iii. The Directorate of ICT shall audit ICT equipment performance every two years and report submitted to the ICT-Directorate for replacement plans.

### 5.1.2 Disposal of Computers

i. Disposal of devices shall not entail Environmental damage or abuse and shall follow disposal instruction manual of the respective Hardware.

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

### 5.1.3 Disaster Recovery and Contingencies

To ensure that internet, data and other mission critical systems do not go down for more than a day:

i. Directorate of ICT shall ensure adequate spares and backup systems shall be maintained and regularly tested for disaster recovery readiness.

ii. All Units of the University are encouraged to take regular backups of their data.

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

## 6.1 INFRASTRUCTURE DEVELOPMENT POLICY

The following policies shall be enforced to ensure that all buildings used for academic and administrative purposes are provided with access to the University's ICT facilities through the provision of data, voice and video points.

### 6.1.1 Existing buildings:

i. The University shall work towards provision of Data points for all offices in existing structures before 2015 to meet the University's strategic plan.

ii. Effective electrical grounding and lightening arrestors shall be provided for existing buildings.

iii. The University shall work towards provision of Data points for all lecture theatres and classrooms in existence before 2015.

iv. The Directorate of works and Maintenance shall ensure that the grounding and lightening arrestors of buildings are regularly tested.

6.1.2 New buildings:

New buildings (Offices and classrooms) shall make provision for:

i. Data, video and telephone points
ii. Electrical grounding and lightening arrestors

## 7.0 SOTFWARE POLICY

The following policies shall govern the acquisition and use of software in the University.

7.1 Pirated or Unlicensed Software:

No pirated or unlicensed software shall be installed on individual workstations or on servers.

7.2 Software Acquisitions:

The University shall acquire license application software for effective teaching, research and administration.

7.3 Open Source Software:

The University shall encourage the use of open source software to reduce the cost of licensing of both application and operating system software.

7.4 Operating System Software

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

- Windows Operating System

- Macintosh Operating System
- Linux Operating System

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

7.5 Uninstalling of Software

Uninstalling software should only take place when it is formerly agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time or if removal can be reverse to status quo.

7.6 Copying of Software:

Users are prohibited from allowing outsiders or themselves making copies of software or soft documents other than those provided for in the relevant licensing agreements.

## 8.0 FUNDING OF ICT INFRASTRUCTURE

The funding of the ICT infrastructure will be centralized and monitores by the ICT-DIRECTORATE.

8.1 Funding Windows for ICT:

The proposed sources of funding are:

i. ICT charges from students
ii. Users service charge
iii. Training and support by the Directorate of ICT
iv. Funding and Donor agencies
v. Any other funding window that will be identified by the ICT-DIRECTORATE subject to the approval of the Vice Chancellor.

8.2 Equipment Purchases Budget

i. The ICT-DIRECTORATE shall make annual budget cover equipment purchases, equipment maintenance, software licenses and communications service charges for all ICT infrastructures.

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

iii. The budget will be subject to the approval of the Vice Chancellor.

## 9.0 DATA AND INFORMATION

9.1 Data Confidentiality:

i. Authorized Users have a duty to keep confidential all University data unless the information has been approved for external publication and information provided in confidence to the University by other entities.

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

iii. Breach of confidentiality through accidental or negligent disclosure may expose a user to disciplinary action.

9.2 Copyright infringement:

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

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

9.3 Data Ownership:

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

However, each User Department should have individual ownership of its own data resources, ensure that the data is accurate and backed up regularly.

## 10.0 POLICY ON PROHIBITED USE OF UNIVERSITY'S ICT RESOURCES

The following lists the prohibited acts when using the ICT Resources. Any staff or student found to have violated this policy will be subjected to disciplinary action, and criminal offences will be reported to the relevant government authorities.

10.1 Advertising and Sponsorship:

Paid advertisements are not permitted on any website using the University domain name except with the written permission of the Vice Chancellor.

10. 2 Peer-to-Peer File Sharing (P2P):

Installation or use of peer to peer file sharing software is not permitted on the network. Exceptions for legitimate teaching or research use and must be approved by the Director of ICT, and only where no alternative technology is appropriate.

10.3 No Business Actives:

Authorized users are not permitted to run a business or publish a journal/magazine ICT Resources except with the written permission of the Vice Chancellor.

10.4 Unauthorized Access:

Authorized users are forbidden from gaining unauthorized access or attempting to gain unauthorized access to ICT Resources belonging to the University and other organizations from the University network.

10.5 Pornography:

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

10. 6 Gambling:

Authorized users are not permitted to utilize the University's ICT Resources to gamble.

10.7 Computer Games:

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

## 11.0 INTERNET, ELECTRONIC MAIL (EMAIL) SERVICES AND UNIVERSITY WEBSITE POLICY

The following policies on email shall be enforced on the setup of email accounts and usage.

### 11.1 Internet:

The University shall provide internet facility to enhance learning, teaching, research and administrative functions of the University. The following policies on internet shall be enforced.

#### 11.1.1 Inappropriate sites:

Inappropriate sites will be filtered or blocked. Inappropriate sites include:

i. Materials relating to pornography.
ii. Offensive materials relating to ethnicity, religion and gender.

#### 11.1.2 Downloading:

i. No user may use the University's Internet facility to download or distribute illegal software or material.

ii. Downloading of multimedia-based file will be restricted.

iii. The University's Internet facility shall not be used to propagate any virus or any software that disrupts or damages computer systems

#### 11.1.3 Disclaimer:

The University is not responsible for material viewed or downloaded by users from the Internet.

11.2 Email Subscription:

i. All staff of the University are required to have a Benue State University, Makurdi email account which will be issued in consultation with Registrar 's Office and activated on assumption of duty.
ii. Email accounts shall be created for all registered students of the University.
iii. Upon request and proper authorization guest or visitors to the University shall be temporary email addresses.

11.2.1 Closure of email account:

For Staff:

i. Dismissed staff: The email account shall be closed immediately
ii. Resignation: The email account shall be closed within 6 months.
iii. Retirement: The email account shall be closed based on consultations.
iv. Death: The email account shall be closed immediately.

For Students:

i. Dismissed student: The email shall be closed immediately.
ii. Graduating student: The accounts of graduating students will be closed one month after graduation.
iii. Death: The email account shall be closed immediately.

11.2.2 Standards Required When Using Email:

When using the email or messaging system, users must not send:

i. Angry or Antagonistic Messages- these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures;
ii. Offensive, Intimidating or Humiliating Emails – University ICT Resources must not be used to humiliate, intimidate or offend another person or other on the basis of their race, gender, religion or ethnicity

11.2.3 Mailing Lists:

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

i. The University staff mailing List shall be used to disseminate information to and among staff.
ii. Posting to the University Staff Mailing List shall be restricted to messages from the Vice-Chancellor, Registrar, statutory boards and committees.
iii. All announcements will not be entertained under the University staff list but sent to the appropriate section on the University website.

11.3 Website:

The policy is to ensure that the content of the site conform to the mission and mandate of the university.

11.3.1 Information, Publicity, Protocol and Public Relations (IPPPR) Unit:

IPPPR will be responsible for maintaining the content of the Home page content and announcement sections.

11.3.2 Unit Website Committees:

Each Unit/Department/Directorate/Colleges will setup a committee to manage and oversee the content of their web pages

11.3.3 Hosting of websites:

No entity is allowed to host its website or web-pages outside the University's web server. Were this is deemed necessary permission shall be sought from the Vice-Chancellor.

## 12.0 E-LEARNING AND DIGITAL RESOURCES

12.1 E-learning Resources:

The University shall promote the integration or e-learning to improve the effectiveness of teaching and learning.

This shall be done by:

i. Promoting the development of e-content to address the educational needs of the University.
ii. Ensure continuous training and promoting of in-house e-learning training capabilities in the long-term.
iii. Ensuring and requiring that all students and academic staff are trained on a continuous basis to equip them with the requisite skills to fully exploit the e-learning tools in the various disciplines.
iv. Collaborate and form global e-learning networks with other academic and research interests groups facilitate sharing of e-learning resources.
v. Establishing the appropriate common e-learning platform responsive to academic needs.
vi. Providing greater access to university education through the development of ICT-based distance education.
vii. All departmental past questions should be submitted to directorate for upload to the e-learning management system.

12.2 Digital Resources:

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

The policy requires that

i. All graduate thesis/dissertations approved by the Graduate Board shall be submitted to the Library in soft copies.
ii. Students and staff data should be achieved.
iii. Soft Copies of minutes of all meetings and reports of statutory boards, committees and others shall be deposited at the office of the registrar.

# 13.0 STRUCTURES FOR ICT POLICY IMPLEMENTATION

The responsibility for and management of ICT is 2-tiered:

13.1.1 ICT Policy and Management Committee (ICT-PMC)

The ICT-PMC determines the overall direction of Information and Communication technology at the University, and endorses the policy and guidelines under the counsel of the Director of ICT

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

### 13.1.2 Composition and Terms of Reference of the ICT-PMC

This committee will be composed of knowledgeable people and ICT-users' stakeholders who are willing to contribute significant insights and to actively participate in high-level ICT policy formulation.

The ICT-PMC Committee shall be constituted by the Vice-Chancellor.

The Terms of Reference of the Committee are:

i. To review and advise on ICT policies, plans, projects and activities.
ii. To support in the development and enforcement of ICT standards, policies and procedures in University.
iii. To promote the harmonization of ICT developments and activities engaged by all units of the University.
iv. To identify and promote areas of collaboration with other institutions to advance the use of ICT for teaching, learning and research.
v. Generate revenue for the University through a functional ICT provision and other ICT projects.
vi. Carry out any other function assigned to it by the Vice-Chancellor.

Members of the ICT-PMC will be drawn from the following:

i. Chairman (To be appointed by the VC)
ii. Director ICT
iii. Three nominees from Senate
iv. Representative of ASUU (ASUU Chairman)
v. Representative of SSANU (SSANU Chairman)
vi. Representative of NASU (NASU Chairman)
vii. Representative of Bursary

viii. Students' Union President
ix. Representative of the Registrar (Secretary)
x. Representative of Audit

## 13.2 The Directorate of Information and Communication Technology (ICT)

The Directorate is responsible for:

i. The implementation of ICT Policies, Strategies and ensuring adherence to ICT Standards by the University.
ii. Providing strategic support for all the University's' ICT Infrastructure. These infrastructure cover but is but limited to the management and oversight of:
    a. The Network Operating Centre
    b. The University's backbone network (Structured cabling for building, Fibre network, Wireless network and other equipment) that formed the University's local area networks (LANs).
iii. Internet Access across the campus
iv. Set-up and provide technical support of the University's email services, Portal and Website
v. Design, implement and manage an appropriate university management information system on staff, students, finance, examinations, courses and programmes.
vi. Provide technical support in the setting up of computer laboratories
vii. Promoting the use of e-learning tools and materials
viii. Provide support in training staff and students in ICT skills
ix. Provide ICT Advisory Services to ICT-DIRECTORATE
x. And any other assignment that will be given by the Vice-Chancellor

## 13.3.1 University Library Computers and Network Resources Acceptable Use Policy

The Benue State University Library System provides access to library collections and other information resources for students, lecturers and administrative staff support through its computers and network resources. The intent of this Acceptable Use

Policy is to ensure that facilities and resources are used most effectively to benefit the greatest number of clients. The policy complements similar guidelines from the University, especially those of the ICT Center and beyond, including applicable state and national policies and laws.

Priority Users: BSU students, lecturers and staff are priority users of library computers and networks. Computers and networks may be restricted to priority users. Users with special needs should contact library staff for assistance.

Non-priority users may be asked to relinquish computers and/or discontinue network access at the discretion of library staff.

Academics First: Library computers and network resources are provided primarily to support the teaching, learning, research, and service activities of BSU lecturers, students and staff. Non-academic activities including, but not limited to game playing, Internet telephony and porn viewing are prohibited on library computers and networks. Library users may not be paid for or otherwise profit from the use of any University-provided computing or network resource or from output produced from such use.

Time Limits: Where a limited number of computers and network resources are reserved for dedicated functions, users must observe posted time limits.

Violation of these policies will attract penalties, including but not limited to verbal and written warnings and the loss of library computers and network resources use privileges.

User Authentication: Library user authentication is required to access all BSU Library System computers and network resources. Current students, lecturers and staff should use their individually-assigned IDs to access computers and network resources. Authorized visitors to the library must present a valid photo ID to request temporary access.

User-Owned Equipment: Authorized users, including BSU students, lecturers and staff may connect personal equipment only through the university's Open Network system or to devices, such as USB ports designated for such use. Users may not unplug library equipment or cables for any reason. Use of personal equipment such as extension, adaptor or power cords must not pose a safety hazard for others.

### 13.3.2 University Library

In terms of ICT services, the University Library in collaboration with the Directorate of ICT will be responsible for creating and making available electronic-based library information resources for the purpose of teaching, learning and research. These include e-books, online Public Access Catalogue (OPAC), digital repository, e-journals, information literacy, audio-visual services and CD-ROMs.

It is the University Policy to improve both the efficiency and effectiveness of library operations and services through the implementation of an Integrated Library System (ILS). The ILS will be accessible within and outside the University network.

The University will support the integration of its library information resources with other interested academic and research groups to share and gain access to more information resources. The University will continue to improve the infrastructure that will ensure easy access to ILS.

## 13.4 User Support Unit

The Directorate of ICT has helpdesk office at the ICT Centre to provide support for both staff and students having difficulty in access ICT facilities and services on campus.

i. The ICT Help Desk shall be establish for problems and changes management for users.
ii. Help Desk procedures shall be established for receiving user problems/requests, user name accounts, tracking, problem resolution and escalation.
iii. The ICT Help Desk shall provide customer-oriented ICT services to the user community by receiving problem calls, requests and enquiries and arranging to have them resolved or addressed by the appropriate ICT personnel.
iv. The Help Desk Service shall be available during working hours, Mondays to Fridays, 8: 00am to 4.00pm
v. The Help Desk can be reached either through their Email: (insert email address).

### 13.5 End-User Skills Development

It is the University Policy to ensure and require that all students and staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the ICT resources to enhance the discharge of their functions.

## 14.0 Policy Enforcement

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

A student who abuses the university's computing, information, and communications resources may also be subject to the loss of these privileges and other disciplinary/sanctions.

Individuals will also be responsible for any financial loss to the University that results from inappropriate use of ICT resources.

The Directorate of ICT shall for the purpose of enforcing this policy document audit user compliance from time to time.

14.1 Sanctions:

Violations of this ICT Policy can lead to any of the following actions:

14.1.2 Withdrawal/Suspension of facilities:

The system and network privileges of the user will be withdrawn, suspended or restricted.

14.1.3 Disciplinary action:

Disciplinary action against the user shall be forwarded to the Vice-Chancellor to be dealt with under the University's disciplinary procedures.

The ICT-DIRECTORATE may request that a user be charged for expenses that have arisen as the result of misuse of the ICT facility.

14.1.4 Breaches of the law:

Breaches of the law will be reported to the appropriate security agencies.

## 15.0 AMENDMENTS TO POLICY

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