UNIVERSITY OF NIGERIA

INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

NOVEMBER, 2020

UNIVERSITY OF NIGERIA
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

PREAMBLE:

This is the Information and Communications Technology (ICT) Policy of the University of Nigeria, Nsukka. It is designed to identify the content and depth of ICT infrastructure required to drive excellence in the overall business of the university: student life-cycle management, academic activities (teaching, learning, research and community service), staff records management and general administration of the university. In addition to the above, the policy identifies and proposes processes and systems including manpower (responsibilities), hardware, software, and procedures for efficient and reputable teaching, learning, research, community development and institutional administration of the university.

It outlines robust system for deployment and management of ICT services in the university including online, e-learning, undergraduate, postgraduate and life-long learning aligned to the strategic objectives of the university. It also seeks to develop effective system for strategic resource allocation on an on-going / rolling plan basis, to achieve a robust system of response to university wide evolving priorities in teaching, research, community development and university administration deploying cutting edge ICT Infrastructure. This policy aims to support the aspirations of the university to become a globally competitive and leading centre of excellence. It aims to ensure emplacement/ deployment and operation of an Information and Communications Technology infrastructure that promotes the vision and mission of the University of Nigeria based on ethical best practices.

1.0. GENERAL CONSIDERATONS/POLICY OUTLINES

1.1. ICT Vision:

To transform the University of Nigeria into a world class learning environment, driven by cutting edge and best in the class Information and Communication Technology Infrastructures.

1.2. ICT Mission:

To ensure that all the components of the mission of the university – teaching, learning, research and community service are ICT-driven.

1.3. Purpose of Policy:

In seeking to support/promote the vision and mission of the university, this policy will specifically seek to

1. Secure the deployment and management of a robust uninterruptible high quality ICT facility to drive the entirety of university business.
2. Ensure the integrity, reliability, availability, and superior performance of ICT Systems.

3. Ensure ethical use of ICT Systems for their intended purposes consistent with the principles and values that govern use of other University facilities and services, and in line with global best practices.
4. Provide user-friendly system for support to all users of ICT to ensure best outcomes for all stakeholders.
5. Establish processes for addressing policy violations in line with evolving technologies, changes in user ecosystem and university priorities.

1.4. Scope of the Policy

This Policy applies at all times to all persons (as may be specified following) who use the ICT Systems and Infrastructure of the university, including but not limited to all University of Nigeria students, staff, researchers, exchange scholars and all visitors (including conference visitors), and third party collaborators and vendors. It applies to the use of all ICT Systems and infrastructure, including those managed by the Directorate of ICT as well as facilities provided or administered by all colleges, faculties, institutes, centres, departments and units of the University; and university-based and controlled facilities (including third parties who may be connected to the university network for the duration of such exposure). Use of ICT Systems, even when carried out on a privately owned computer that is not managed or maintained by the University of Nigeria but is connected to the University network or deployed in the implementation of University official business shall be governed by applicable aspects of this Policy.

2.0. GOVERNANCE POLICY

2.1.INTRODUCTION

The trend worldwide is in the direction of decentralized management structure. Accordingly this UNN ICT Governance policy shall provide for regulating, monitoring and the implementation of the university ICT policy at all functional levels of the university.

2.2. STRUCTURE

The Governance Structure of the University ICT shall consist of:

(a) The ICT Management Board
(b) ICT Technical Committee
(c) The ICT Centre
(d) The ICT Units
(e) All other ICT related centres of the university

(See Appendix I: The organogram of the ICT structure)

2.2.1. THE ICT MANAGEMENT BOARD.

The membership of Board shall consist of the following:

1. A chairman that shall be a member of the University Governing Council to be appointed by the Council
2. The Vice-Chancellor or his representative
3. The Bursar or his representative
4. The ICT Director
5. The Directors of ICT-related Centres
6. The DVC, UNEC or his representative

7. The Provost, College of Medicine or representative
8. Two honorary external members appointed by the Vice Chancellor. Such persons shall be nationally and internationally acknowledged leading experts in ICT matters and shall also be disposed to assist the management board to secure grants, aids and endowments for ICT

The Board shall be responsible for the monitoring and implementation of the ICT policy with the following as its specific functions:

(i) Proposing policy options in relation to development plans, fund raising strategies, regulations enactment, etc.
(ii) Monitoring the role of players in the policy.
(iii) Liaising with industry, NUC, Ministry of Education, NCC,NITDA and others on ICT matters.
(iv) Representing the stakeholders in all ICT concerns owned by the university, or in which the university has interest.
(v) Ensuring the compliance of all stakeholder to the ICT policy
(vi) Advising the University management on changing financial implication of maintaining cutting-edge ICT infrastructure and also on possible funding sources and variations including all embedded staff and student contributions/charges
(vii) Superintend the implementation of the Budget of the ICT directorate to ensure seamless and high quality ICT service

2.2.2. ICT TECHNICAL COMMITTEE

For effectiveness, there shall be an ICT Technical Committee to assist the Board on all technical matters. The Technical Committee shall consist of the following:

1. Director, ICT Centre (Chairman)
2. Deputy Directors, ICT Centre
3. Head, Computer Science
4. Head, Electronics Engineering
5. Directors/Heads of other ICT related Centres and Departments
6. Representative of the University Librarian

The functions of the Technical Committee shall include but not limited to the following:

1. To study emerging technologies and propose integration into university ICT resources given current needs
2. Defining the functional relationship among all ICT related units and ensuring that there are no duplications of functions or redundancy among them.
3. Supervise the development of a functional handbook for the relevant ICT related Centres and day to day implementation of aspects of this policy as may be advised by the management board
4. To ensure that issues of safety, scope, privacy, copyright and liability are identified and managed in the best interest of the University
5. To ensure sustainable development and emplacement of high quality infrastructure and management processes in line with technology evolution, user ecosystem changes and global best practices

6. Liaise with all heads of departments, units and centres to identify ICT policy violations and report same to the Board.
7. Advise the ICT Management Board on all aspects of the development of the University ICT infrastructure.
8. Advise the ICT Board on manpower and training/ capacity needs for the maintenance of robust cutting edge ICT infrastructure.
9. Advise the University management on matters related to third party and contractor / vendor service provisions related to ICT bearing in mind the critical need to ensure technology transfer to responsible University ICT staff over the minimum possible timelines. In this regards, it is recommended that:
    a. third party / contract ICT service to the University be transferred to the University not later than 5 years from first provision of such service;
    b. appropriate number of university ICT personnel shall have been trained over the contract period; and
    c. wherever necessary, appropriate after sales support in favour of the university shall be negotiated as part of the initial service / equipment contract.

2.2.3 THE ICT CENTRE

The ICT Centre, in carrying out its duties, shall:

1. Be responsible for the Planning, Designing, Implementation, Co-ordination, and Monitoring of the implementation of all ICT projects which includes, but not limited to deployment, operation, maintenance, support and disposal functions.
2. Superintend the overall development of ICT in the University. This is to ensure the effective and optimal utilization of ICT resources in the University.
3. Superintend the overall management of the university ICT infrastructure as to ensure the efficient and effective use of the University's ICT infrastructure
4. Ensure considerate use of infrastructure and facilities by competing users.
5. Drive the training, continual retraining, certification and motivation of appropriate level (quality and quantity) of ICT personnel and professionals needed to maintain a very efficient and robust infrastructure for set purpose
6. Advise the University and all units thereof (including research personnel who procure ICT equipment as part of university-based grant-funded activities) on all matters related to procurement of all ICT equipment to ensure equipment compatibility, ease of maintenance and value for money.
7. Establish and maintain highly trained, competent and motivated equipment maintenance crew to:
    a. Achieve timely, seamless and cost-effective maintenance of all of University’s ICT equipment
    b. Ensure there is kept a roaster/timetable for such maintenance and
    c. Undertake the maintenance of ICT equipment and infrastructure
8. Develop and implement an appropriate backup and restoration policy for all University Institutional Data, a business continuity plan and information security policies to ensure protection, integrity and reliability of all institutional data.
9. Promote and implement the development of a centralized system of authentication that ensures users of the University’s information technology resources and associated data

are correctly identified, authorized and authenticated before access to the corresponding systems and resources is granted.

10. Ensure the development and implementation of appropriate protocol to ensure audit trail to track access to all Confidential and Highly Confidential Institutional data.

11. Ensure that whenever certain portion of a given institutional data is generated and maintained by an external party, there is a mechanism to track and account for any fees that may be attached to such actions as should duly accrue to the University for the period of such a contract/ arrangement

For purpose of this Policy, the ICT infrastructure of the University shall be understood to include all computer hardware (howsoever defined) including handheld devices and peripherals, wired or wireless network equipment owned by, and administered by or for or licensed to the University; software licensed to, owned by or howsoever operated by the University or for the University legitimately; and any other facilities related to the foregoing, owned by, licenced to, or otherwise legitimately operated by the University (or her agents and proxies) for purpose of or in pursuit of this policy.

The ICT Centre shall be divided into the following units, each of them headed by Deputy Director or such other competent professional of significantly high rank. The units are:

1. Administrative Unit
2. Network unit
3. Hardware and Maintenance unit
4. Software unit
5. Capacity building unit
6. E-learning unit
7. Computer Based Testing (CBT) unit
8. Customer services unit

2.2.4 ALL OTHER ICT RELATED CENTRES

These centres shall include:

i. Computing Centre
ii. Management Information Systems Unit
iii. Centre for Distance and e-Learning
iv. Centre for Lion Gadgets and Technologies
v. Computer Communication Centre
vi. Any other centres that may be created or defined by the appropriate authorities for purpose of this policy.

3.0 RESPONSIBILITIES OF ICT UNITS

The responsibilities of the individual units of the ICT Centre shall be as follows:

3.1. ADMINISTRATION UNIT

Manage the Office of the Director and the Central Administration of the ICT Centre, and coordinate the different units.

3.2. NETWORK UNIT

i. Design, implement and maintain the university network infrastructure (the backbone, the LAN, the Intranet, the Wireless, etc.)
ii. Determine the cost of bandwidth relevant ISPs and advise accordingly.
iii. Deploy, manage and efficiently utilize available bandwidth to best achieve set objectives of the University.
iv. Develop a network map showing the network layout throughout the university campuses

3.3. HARDWARE UNIT

i. Determine and schedule periodic preventive maintenance of all university ICT hardware
ii. Determine cost of maintenance of equipment and facilities and therefrom conduct a periodic review of any embedded costs, charges and contribution (including ICT cost component of funded University-based research).
iii. Determine cost of replacement of equipment and procurement of new additional ones.

3.4. SOFTWARE UNIT

i. Determine cost of software licenses (application for the main information systems, specialized applications, database platforms, web and desktop applications, antiviruses) including common applications procured based on multi-user licence etc., and advise accordingly
ii. Design, implement and maintain the university website, portals and in-house software solutions
iii. Manage university data.

3.5. CAPACITY BUILDING UNIT

i. Identifying and implementing relevant ICT training programmes for all cadres of the university staff.

ii. Ensuring that every staff make use of available ICT resources in carrying out their official duties.

3.6. E-LEARNING UNIT

i. Provide the infrastructure for online activities such as meetings, collaborations, webinars, teaching and learning, etc.
iii. Train staff and students on how to access and use necessary online platforms

3.7. CBT UNIT

i. Provide the necessary infrastructure and technical support for all computer-based tests and examinations in the university.

iv. In consultation with departments and the Exam Unit of the Registry department, provide timetables for all CBT tests and examinations

3.8. CUSTOMER SERVICE UNIT

i. Provide support to all categories of users of ICT resources.

ii. Escalate user feedbacks to relevant ICT units for immediate action

4.0. ICT SERVICE MANAGEMENT POLICY

4.1. DEFINITIONS

4.1.1. PRIVACY, DATA SECURITY & INTEGRITY

Institutional data refers to all data created, collected, maintained, recorded or managed by the University and/or agents working on her behalf, which satisfy one or more of the following criteria:

- The data is relevant to planning, managing, operating, or auditing a major administrative function of the University.
- The data is referenced or required for use by more than one organizational unit
- The data is included in an official University administrative report
- The data is used to derive a data element that meets these criteria.

This data can be contained in any form, including but not limited to documents, databases, spread sheets, email and web site; represented in any form including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof; communicated in any form including but not limited to handwriting, printing, photocopying, photographing and web publishing; and recorded upon any media including but not limited to papers, maps, films, prints, discs, drives, memory sticks and other computing devices. These data may take the form of one or more of the following:

a. Research Data refers to all outputs of creative work undertaken on a systematic basis in order to create knowledge and increase the stock of knowledge and information. These include all original research publications (books, book chapters, Journal articles, conference publications, thesis and dissertations), projects / annual reports, planning documents (policies, strategic plans) etc.

b. Library Data refers to data, which contain information on University library profiles such as subscribed journals, available print collections (books, serials and references), available special collections (photos, music, archives).

c. Academic Data refers to data, which contain information on University academic profiles such as courses/curricula enrolment, results, degree/ transcript, course /examination time-tables all related academic document and alumni related data bases.

d. Student Data refers to information relating to student characteristics (course & residence registration, academic performance financial status) and student demographics (region, age, sex, religion).
e. Human Resource Data refers to data, which contain information on the human resource profile of the University such as establishment, staffing level, procedures and manuals, benefit schemes and beneficiaries.
f. Personnel Data refers to information relating to staff characteristics (qualification, rank, pension accrued, compensations, salary, financial and banking and insurance etc.) and staff demographics (region, age, sex, religion, marital status, department and all personnel related data and documents, etc.).
g. Financial Data refers to data, which contain information on University financial profiles such as revenue, expenditure, budget, assets, liabilities, contracts, including academic contracts and facilities.

Members of the University community and other (third party) stakeholders require access to different categories of institutional data in support of the University's teaching, research and community service. Members of the above community working with or using institutional data in any manner must comply with all applicable international conventions, national laws on data protection and all applicable University policies, procedures and standards, as well as all applicable contracts and licenses. To enable clear application of appropriate policies institutional data may be categorised according to roles and controls as follows:

- **Data Owner** – a unit or official with management policy and operational responsibility for institutional data.
- **Data Custodian** – a unit or employee responsible for the operation and management of systems and servers which collect, manage and provide access to institutional data. Thus, the director ICT, including its staff is responsible for managing the server infrastructure that houses the academic data or other data as may be consigned to the unit by the University.
- **Data user** – a member of the community using institutional data in the conduct of University business.

The Data owners as defined are responsible for the formal classification of such data based on its sensitivity and confidentiality and thus for purposes of data security. Sensitivity and confidentiality of data relate to challenges that may arise from loss of data or data falling into unauthorised hands as: loss of critical University operations; loss of opportunities, cost or value of the data; damage to the reputation of the university (including members of University community) that may arise or lead to litigation and financial loss; lack of corrective actions or repairs and violation of University mission and policies. To manage these challenges data may be categorised and managed as follows:

Highly Confidential: Data is classified as Highly Confidential when an unauthorized disclosure, alteration or destruction of that data will cause a significant level of risk to the University or members of the community. Access to Highly Confidential data must be responsibly and individually requested and then authorized by the Data Owner who is responsible for the data. The assessment of risk and access approval will be determined by the data owner or appropriate University functionaries (and in consultation with private

owner as appropriate). Examples of such data include sensitive health information, personal data including banking and financial information, university financial data and information, sensitive student personal information and all data protected by law. Such data may not be sent by email or forwarded. Confidential printing and hand/ signed delivery and required to transmit such data. Electronic encryption is needed for electronic transmission.

Confidential: These relate to information that would not necessarily expose the University to significant loss, but the data owner has determined security measures are needed to protect from unauthorized access, modifications, or disclosure. Examples include Intellectual Property related data: licensed and/ or under development, records, purchasing information, vendor contracts, and system configurations and data protected by law or whose release may only follow FOI act requests. As for Highly confidential data above, these may not be transmitted via email (particularly to an external email).

Internal use data: These relate to data classified as internal / private for all the information assets that are not explicitly classified as Highly Confidential, Confidential or Public data. A reasonable level of security control should be applied to internal data. Such data may be routinely available without restriction but its integrity must be carefully maintained. Examples include routine correspondence, employee newsletters and memos, inter-office memoranda, internal policies & procedures. No special precautions are needed for transmission of these data.

Public Data: Data will be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to the University and its affiliates. Such data are intended for broad distribution in support of the University's missions or freely available to any person or organization with no restrictions. Examples include brochures, news releases, pamphlets, web sites, internal phone directories, marketing materials. No special precautions are needed for handling and transfer.

The University shall ensure that information relevant for tactical and strategic needs of University management is provided in a timely and easy to access way. The University shall therefore, promote and support the development of high level reporting applications that consolidates data from across all institutional databases using data mining and/or other approaches that support development and management of secure audit trail.

4.2. ACCESS ETHICS

The ICT Unit shall grant internet access (and university specific email account) to the University network to:

Staff:

All staff of the University shall be provided with valid Internet access and email accounts for official or authorised personal uses. These accounts shall remain active as long as the staff is in the service or pensioner of the university. In the event of resignation or dismissal the staff shall be given a grace period of 6 months to back out his emails.

Students:
All registered students of the University shall be provided with valid Internet and email accounts to enhance lawful use in the pursuit of their studies. Such account shall be disabled one year after graduation.

Administration:
These accounts are applicable to Principal Officers of the University, Provost, Deans/Directors, Heads of Departments and Units and other university functionaries for official use where it is necessary to identify an office or action rather than an operative. Such accounts shall be transferred to in-coming officers at times of change in administration.

Visitors:
These are temporary accounts which shall be given to intending users who are in the University for Official Duties or other short duration activities e.g. external examiners, visiting staff/scholars, conference visitors and visitors from other institutions. Application for this category of accounts must be through the head of department or unit to which the visitor is affiliated. Such an account shall be disabled immediately the visitor leaves the university based on a time.

Restrictions to Access:
Users are expressly forbidden from unauthorized access to accounts, data or files on University ICT resources. The Director of ICT may restrict access to an individual user on the grounds that the user is in breach of this policy.

University Liability:
The University accepts no responsibility for:
a. Loss or damage or consequential loss or damage, arising from personal use of her ICT resources (including if such loss or damage were to arise from authorised access);
b. Loss of data or interference with personal files arising from the University's efforts to maintain her ICT resources. Users are advised to constantly backup their personal and important data and specifically to desist from storing personal data and files on university ICT facilities.

4.3. CODE OF CONDUCT AND OPERATIONAL ETHICS FOR ICT STAFF
ICT Centre (including all staff and third party personnel) shall follow a policy of conducting its business ethically and in compliance with the letter and spirit of the law and international best practices. This is critical to international reputation for excellence and integrity of the University of Nigeria.

4.3.1. SERVER ROOM/DATA CENTRE

a. Physical Access:

i. Access to this facility is restricted to only authorized personnel of the ICT Centre or any other authorized third-party personnel as may be determined by the Director of ICT.
ii. All third-party access to the server room/data centre shall be supervised by the staff responsible for that centre
iii. Edibles, liquid, electromagnetic objects or any other objects that may constitute hazard to the data centre/server room equipment or their functions are not authorized to be brought into the server room/data centre by anyone.
iv. A log of all entrants into the server room/data centre must be maintained at all times and backed up by secure CCTv records

b. Movement of equipment

Unauthorized movement of equipment in and out of the server room/data centre is strictly prohibited.

c. Physical protection

The server room/data centre shall be protected against exposure to water, Dust, fire, electrical surge and high temperature

4.3.2. DATA PROTECTION

All ICT staff shall ensure the protection of the university digital infrastructure and information assets against any compromise or attack that may affect its confidentiality, integrity or availability. To ensure this the following steps need to be taken:

a. Access privileges to user accounts, official correspondences and documents must not be abused.
b. Copying, divulging or any other form of manipulation of official documents is prohibited.
c. All ICT infrastructure must be protected from virus, malware, etc. with necessary tools.

4.3.3. SPECIFIC DAY TO DAY OPERATIONS AND OTHER RESPONSIBILITIES OF THE ICT CENTRE

In the conduct of its day-to-day operations, the ICT Centre shall see to the following:

i. Integrity, maintenance and efficiency of the campus Network
ii. Network infrastructure including internet servers, switches, routers, optic fibres, wireless access points, etc.
iii. Intranet/Internet Access
iv. Provision and management of university email (…@unn.edu.ng)
v. Provision of Internet Service on campus
vi. Maintenance of all servers connected to the network
vii. Internet Security management and system integrity
viii. Maintenance of network infrastructure in all buildings on campus
ix. CISCO Administration.

x. Development of such software as may be directed or required for effective operation of the University ICT and System-wide enterprise management
xi. Administration of staff and students Records
xii. Student life cycle management including management of processes for timely issuance of transcript
xiii. Production of staff and students Identity cards
xiv. Administration of University portal and Database servers
xv. Collaboration with the Registrar/Faculties and Department to implement course registration and process results; implementing all online registrations
xvi. Collaboration with the Bursar to ensure comprehensive fees collection across the system and financial management as may be required
xvii. Collaboration with Departments and Faculties/the Registrar to produce Examinations Time-Table and ensure seamless management of semester and professional examinations
xviii. Collaboration with Departments to implement CBT examinations
xix. Collaboration with Personnel Services to manage staff database
xx. Collaboration with Medical Centre Services for Hospital Enterprise Management
xxi. Collaboration with the University research community and students to enhance research visibility
xxii. Collaboration with appropriate organs of the University including but not limited to the University Senate to achieve enhanced visibility and ranking for the university
xxiii. Creation of sub-domains and populating them for departments, faculties and centres
xxiv. Maintenance of Portal and Database servers
xxv. Administration of Web servers and Content Management System.
xxvi. Installation and management of University computing facilities/data processing and analysis, graphics services and facilities as well as sales and services; and provision of commercial access to same as may be determined by the university from time to time
xxvii. Organizing ICT Training Programme for both staff and students
xxviii. Organizing Professionals certification training programmes such as CISCO Training
xxix. Deploying multimedia systems for seminars, conferences and workshops
xxx. Deploying multimedia systems in all lecture rooms and auditoria
xxxi. Deploying multimedia systems for post-graduate theses defense on request.
xxxii. Ensuring ethical use of all University ICT infrastructure including by constraining or otherwise denying access to sites and services not deemed consistent with the business of the University
xxxiii. Other ICT related services as may be identified or defined from time to time by the University

4.3.4. PROTECTION OF OTHER ICT PHYSICAL INFRASTRUCTURE

It shall be the responsibility of the ICT Centre to work with appropriate organs of the university (Works, Physical planning, Security, etc.) to ensure the protection of all ICT infrastructure including fibre optic cables, masts, radios; provision of cabling maps and marks, etc. However, it is the responsibility of the host department, centre, office, hostel, etc. to ensure the security of any ICT infrastructure installed within their premises

4.4. RESPONSIBILITY OF OTHER USERS

It shall be the responsibility of other users to:

a. Ensure that a secure backup is kept of all their data and that a backup alternative exists in the event of failure of a piece of technology in the network; and
b. Ensure that they have been checked against the intended purpose prior to commencement of usage. However, where ICT Infrastructure is being used in such a way that the content or subject matter of the use is sensitive or likely to raise questions related to unethical or inappropriate use of ICT infrastructure, the user shall take appropriate steps to ensure that:
    i. no members of the University community or any other people are exposed to materials that may cause offence; and
    ii. there is no breach of any laws regarding the viewing, use or publication of materials.
c. The University shall accept no responsibility for any emotional or mental harm resulting from using the University's ICT Infrastructure.

5.0. DEVELOPMENT OF THE UNIVERSITY ICT INFRASTRUCTURE:

It shall be the responsibility of the Directorate of ICT to:

a. Maintain and update a **short**, **medium** and **long-terms development** plan for this purpose. These plans shall encompass all aspects of hardware and software procurement, installation, commissioning and maintenance as well as development of requisite manpower in line with the evolution of technology, evolving demands of the University and funding requirement
b. Advise the University management on matters related to third party and contractor/vendor service provisions related to ICT bearing in mind the critical need to ensure technology transfer to responsible University ICT staff over the minimum possible timelines. In this regards, it is recommended that:
    i. third party/contract ICT service to the University be transferred to the University not later than 5 years from first provision of such service;
    ii. appropriate number of university ICT personnel shall have been trained over the contract period; and
    iii. wherever necessary, appropriate after sales support in favour of the university shall be negotiated as part of the initial service / equipment contract.
c. Drive the transition from the current wireless network to a combination of wired and wireless network to increase speed, reduce down time and maintenance needs and achieve long-term economy.
d. Develop timetables for the phased and gradual fixed wire cabling of all University facilities, starting first with permanent structures. Such cabling shall include the cabling of all offices, laboratories and workshops to enable seamless communication and reduced labour down-time in the university.
e. Advise the University and take necessary action as directed for the disposal of all end of life ICT equipment in line with national policy, global best practices and

specific environmental considerations bearing in mind the need for data protection (The Privacy and Personal Information Protection Act 1998; The Health Records and Information Policy Act 2002) and social responsibility

It is expected, subject to availability of resources that implementation of items **a-e** shall commence immediately and run in phases over the short term (4-5 years) and medium term (10 years) based on carefully considered grouping and prioritization of University facilities and resource availability.

To ensure that the need for cabling fall out with the completion of cabling of existing facilities, all new structural developments of the University going forward shall include bill for comprehensive cable installation as part of construction.

5.1. ICT BUDGET

The University shall make provision for effective and seamless funding of ICT services based on total personnel and bandwidth availability needed to provide unlimited high-speed access to the university community as well as for on-going provision of all necessary ICT infrastructures. This should be done on a continuous rolling plan bases. Students and staff shall pay annual subscriptions for ICT services as may be approved by the administration. All charges for the ICT services shall constitute the base or minimum provision to the annual budget for the ICT directorate. The university can augment this in the event of shortfall on required expenses. This shall be strictly dedicated for the provision of ICT services in the university.

This fund shall be disbursed as directed by the Management Board of ICT to ensure high quality ICT services to the university. Accordingly, it is recommended that a minimum of N12,00.00 per person per annum shall be invested into ICT by the university. This shall be revised at least once every three years to accommodate changes in cost of provision of ICT services. Typically, this fund shall be deployed as suggested in Appendix II.

5.2. SHORT TERM ACTIONS IDENTIFIED AND RECOMMENDED (1-5 YEARS)

The ICT Centre in collaboration with the relevant arms of the University Management shall carry out the following:

1. Complete, commission and equip the dedicated purpose-designed University Data Centre Facility to enable consolidation of University Data and ICT Infrastructure in a secure facility that shall also provide enough space to enable robust development of this vital organ of the university
2. Initiate action to achieve gradual and phased network and telephony cabling of all university permanent structures based on prioritization of such facilities for utility, cost effectiveness, user needs, staff and student density, etc.
3. Ensure without delay that on-going and uncompleted university structures are adjusted to include data and telephony cabling where that is not already in the bill
4. Develop and commission a VoIP system to enable voice communication across the system (particularly while the cable development is in progress).

5. Take action to extend Optic Fibre Cabling (OFC) and wireless network to all parts of the university that are currently not reached. Efforts should aim to bring internet to all classrooms, teaching laboratories, studios and workshops (prioritizing classes and facilities that hold 100 students and above) to enable proper use of the smart boards that may be approaching end of life without being used at all.
6. Invest in solar or at least simple battery backup for wireless services to reduce down time due to power failure (to all classrooms) and also provide inverter systems to support smartboards.
7. Invest in student class attendance management software and hardware to enable management of classroom and lecture participation, particularly for large classes
8. Have a programme for training of ICT staff that makes it mandatory for every staff from level 7 and above to be sponsored by the University to, at least, one training/workshop every year.
9. The university should sponsor ICT staff from level 13 and above to their professional body's annual conference every year. University shall be encouraged to pay their annual membership dues for at least one professional body per year
10. To carry out item 8 effectively, MOUs with vendors on ICT matters should include a section that mandates the vendor to sponsor at least 5 ICT staff to conferences and workshops annually.
11. Embark on training and retraining of all categories of ICT personnel to achieve various forms of certification and improve motivation. There should be strict timelines for the retraining and certification of all ICT personnel.
12. Deploy appropriate online and e-learning programs and platforms and continual training and retraining of academics and support staff
13. Continual audit of ICT infrastructure to achieve improvement across the system. This should be an on-going action

5.3. MEDIUM TERM INVESTMENT (6-10 YEARS)

1. Procurement and installation of high performance computing facilities to aid high speed computing and drive high-end research, collaboration and commercial applications. This will be installed in the data centre built for that purpose
2. Extension of optic fibre and cabling to cover all offices, classrooms, reading rooms, laboratories, workshops studio and buildings in the university not covered in the first phase of cabled network development. This should be concluded in the first half of this phase
3. Continued training and retraining of ICT personnel
4. Implementation and expansion of online and e-learning platforms, programs and facilities to more programmes and courses
5. Continual audit of ICT infrastructure to achieve improvement across the system

5.4. LONG TERM DEVELOPMENT AND MANAGEMENT OF THE UNIVERSITY ICT INFRASTRUCTURE (> 10 YEARS)

It is expected that the ICT Infrastructure of the University shall evolve into a robust facility to support the development of the University to a globally acclaimed centre for knowledge creation and transfer. The facility shall integrate voice, data and video, to form a unified information technology resource to drive all of the University's businesses for the entire university community. The ICT Centre shall chaperon this development by monitoring global developments in this area and advising University management as appropriate. To achieve the above, the following actions shall be continuously implemented:

1. Benchmarking of ICT infrastructure to global best practices
2. Development of possibilities for generating funds through advanced computing capacity and resources
3. Training and retraining of personnel
4. Provision of internet service beyond the community on commercial basis by deploying excess capacity for revenue and Cooperate Social Responsibility (CSR)

6.0. POLICY ENFORCEMENT, VIOLATION AND SANCTIONS

i. Complaints of Alleged Violations

An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established and appropriate University procedures for students, academic staff, and non-teaching staff. The individual is also encouraged to report the alleged violation to the Authority (ICT) overseeing the facility most directly

ii. Reporting Observed Violations

If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Authority (ICT or other owners) overseeing the facility most directly involved

iii. Disciplinary Procedures

Alleged violations of this Policy will be redressed in accordance with appropriate disciplinary procedures for academic staff, non-teaching staff, students or other approved users as applicable.

iv. Penalties

Individuals found to have violated this Policy may be subject to penalties provided for in other University policies dealing with the underlying conduct.

v. Legal Liability for Unlawful Use

In addition to University disciplinary procedures, users may be subject to criminal prosecution, civil liability, or both for unlawful use or abuse of any ICT System and Infrastructure provided that such persons shall be able to appeal or request for reconsideration of disciplinary processes in accordance with the extant regulations of the University.

7.0. CONCLUSION

This document is compiled, signed and presented this **4th Day of November 2020** by the **Technology and Information Governance Sub-Committee** of Council Strategic Planning Committee, comprising the following members of staff of the University of Nigeria:

Signed:

1. Prof. Jerry Ugwuanyi – Chairman _____

2. Mr. Paul C. Oranu – Member _____

3. Rev. Fr. Edward Anoliefo – " _____

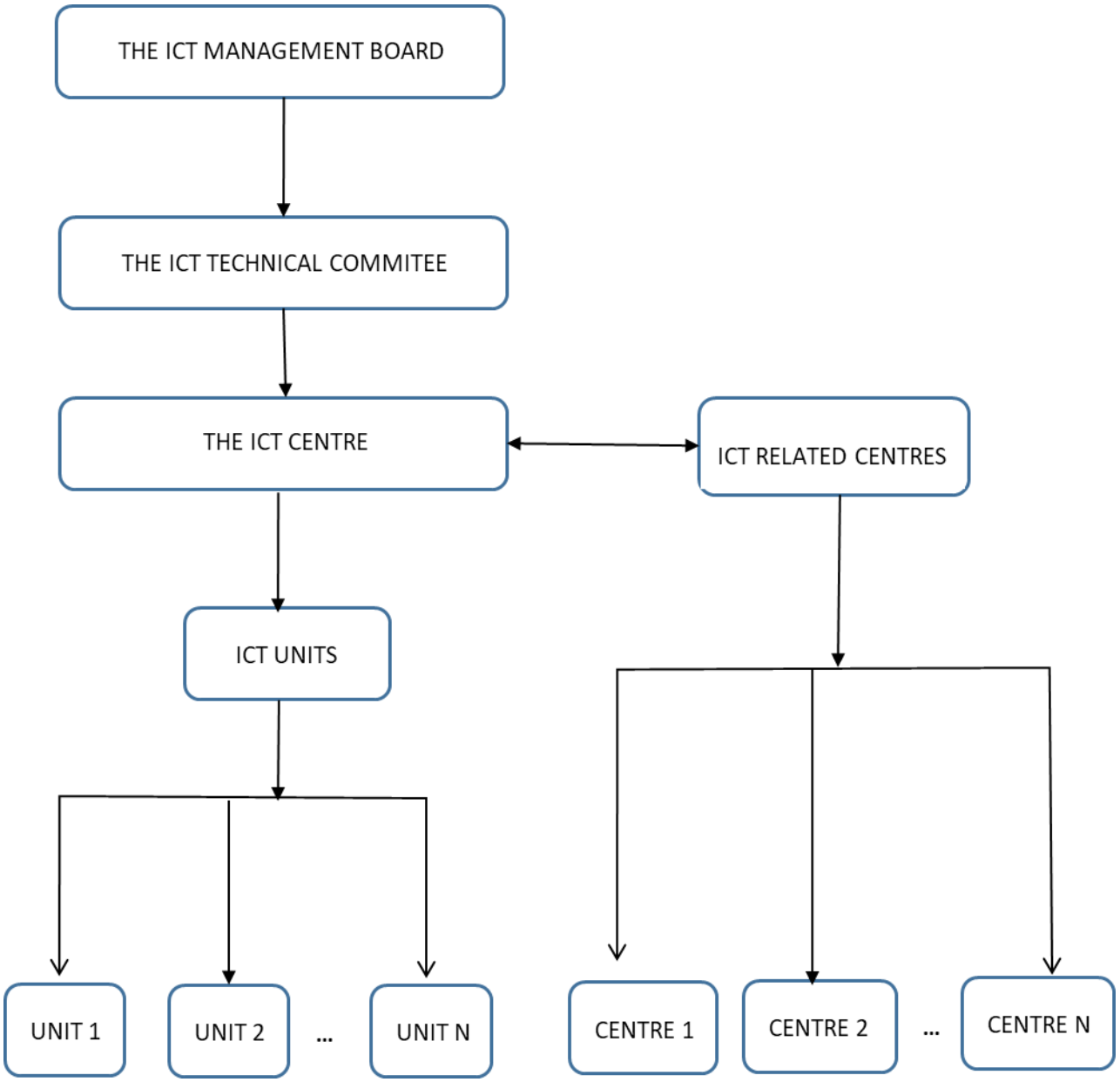
4. Mr. Lazarus Ekeke – " _____

5. Dr. Collins Udeano – " _____

6. Engr. Chidubem Obaraegwu – " _____

7. Mr. Gaius C. Ebere - Secretary _____

APPENDIX A
ORGANOGRAM OF THE ICT STRUCTURE



APPENDIX B:
ICT ANNUAL BUDGET STRUCTURE

UNIVERSITY OF NIGERIA DIRECTORATE OF ICT INFRASTRUCTURAL BUDGET					
1: ICT INFRASTRUCTURE COSTING (EXPENDITURE)					
S/N	**`**	**SERVICE DESCRIPTION**	**UNIT**	**AMOUNT PER QUARTER**	**TOTAL COST ANNUALLY**
A:	**Bandwidth resources**				
1		1 STM (155 mbps) for UNN Nsukka Campus	Per Quarter (3 Months)	12,615,999.01	50,463,996.04
2		1 STM (155 mbps) for UNEC & College of Medicine	Per Quarter (3 Months)	12,615,999.01	50,463,996.04
3		Category A: 1 STM (155 mbps) UNN	Per Quarter (3 Months)	7,150,000.00	28,600,000.00
					129,527,992.08
B:	**Network resources**				
1		Network Routers	20	650,000.00	13,000,000.00
2		Network Switches	80	350,000.00	28,000,000.00
3		Wireless Radios	100	170,000.00	17,000,000.00
4		Fiber Links	Lot	55,000,000.00	55,000,000.00
5		Network Cable Cat6	80	120,000.00	7,200,000.00
6		Networking Tools	Lot	4,000,000.00	4,000,000.00
					124,200,000.00
C:	**Power backup**				
1		10KVA Inverter with Batteries for Data Centres Plus Solar Panels	3	12,000,000.00	36,000,000.00
2		1.5KVA Inverter with Batteries for Mini-pups Plus Solar Panels	18	1,300,000.00	23,400,000.00
					59,400,000.00
D:	**Servers & laptops**				
1		PowerEdge R740 Rack Server	4	4,500,000.00	18,000,000.00
2		Corei7 Laptops	10	600,000.00	6,000,000.00
3		HP Core i5	500	320,000.00	160,000,000.00
4		Hp Color LaserJet Pro MFP M479fdw All-In-One Auto Duplex Printer	2	420,000.00	840,000.00
					184,840,000.00
E:	**Software resources**				
1		Window Server 2019 Operating System Enterprise	3	450,000.00	1,350,000.00
2		Window 10 Operating System Professional	3	150,000.00	450,000.00

3		Office 2019 Educational License	3	230,000.00	690,000.00
4		Norton 360 Deluxe	3	240,000.00	720,000.00
5		Hospital Management System	Lot	45,000,000.00	45,000,000.00
6		Human Resources Management System	Lot	50,000,000.00	50,000,000.00
7		Document Management System	Lot	40,000,000.00	40,000,000.00
					138,210,000.00
		TOTAL			**636,177,992.08**
F:	**Staff development**	Staff training (Local & International)	Lot	**5% of TOTAL**	31,808,900.00
G.	**Contingency**		Lot	**5% of TOTAL**	31,808,900.00
H.	**System-wide vote**		Lot	**1.59% of TOTAL**	10,102,103.96
I.	**Transport & Logistics**		Lot	**1.59% of TOTAL**	10,102,103.96
		OVERALL TOTAL			**720,000,000.00**

2: ICT INFRASTRUCTURE FUNDING SOURCE (INCOME)					
S/N	**FUNDING SOURCE**	**DESCRIPTION OF SOURCE**	**QUANTITY (PERSON)**	**AMOUNT**	**TOTAL AMOUNT ANNUALLY**
A	**Internal:**				
1	Student Year 1	ICT fees	10,000.00	12,000.00	120,000,000.00
2	Postgraduate students		12,000.00	12,000.00	144,000,000.00
3	Student Other Year	ICT fees	35,000.00	8,000.00	280,000,000.00
4	Senior Staff	Deduction from Salaries @ 2,000 per Staff	8,318.00	16,636,000.00	199,632,000.00
5	Junior Staff	Deduction from Salaries @ 1,000 per Staff	1,100.00	1,100,000.00	13,200,000.00
B	**Federal Government Agencies:**				
1	Tertiary Education Trust Fund	Supply of ICT Equipment and Others	Nil	0.00	0.00
2	National Information Technology Development Agency (NITDA)	Supply of ICT Equipment and Others	Nil	0.00	0.00

3	Nigerian Communication Commission (NCC)	Supply of ICT Equipment and Others	Nil	0.00	0.00
4	Petroleum Technology Development Fund (PTDF)	Supply of ICT Equipment and Others	Nil	0.00	0.00
5	Other Federal Grants	Supply of ICT Equipment and Others	Nil	0.00	0.00
		TOTAL			**756,832,000.00**