BAYERO UNIVERSITY, KANO

ICT POLICY

December, 2020

FOREWORD

Today, Information and Communications Technology (ICT) has become an indispensable enabling tool for progress of organizations, particularly, Higher Educational Institutions (HEIs). It is a technology that is used for the processing and distribution of data/information using computer hardware and software, telecommunications, and digital electronics.

ICT resources remain central to University functions, activities and roles. Its application and usage requires coordination from a central unit, and the Centre for Information Technology (CIT) has been saddled with this responsibility. The Centre was established with the mandate of promoting Information Technology in teaching learning and research, providing management decision support, deploying and maintaining IT infrastructure in Bayero University Kano.

Consequent upon this, the Bayero University Kano has set out this ICT policy as an underlying guideline for proper monitoring and control towards ensuring efficient and effective use of ICT facilities to achieve its mission and vision. This ICT policy document therefore articulates policy guidelines and framework as programmes of action that will guide the University in the development and application of ICT facilities by all units of the University for the support of teaching and learning. This will be achieved by integrating ICT into teaching, learning, research, information dissemination and management of activities to close the knowledge and technology gap that hitherto exists within the system and place global information grid at the disposal of the University community.

Prof. Sagir Adamu Abbas, FMAN
Vice Chancellor,
Bayero University Kano

List of Abbreviations and Acronyms

ARIS	**:**	Academic Records Information System
AKCDR&T	**:**	Aminu Kano Centre for Democratic Research and Teaching
AKTH	**:**	Aminu Kano Teaching Hospital
CIT	**:**	Centre for Information Technology
DC	**:**	Data Communication
DLE	**:**	Digital Learning Environment
DNS	**:**	Domain Name Service
Email	**:**	Electronic Mail
FINIS	**:**	Financial Information System
FTP	**:**	File Transfer Protocol
HURIS	**:**	Human Resource Information System
ICT	**:**	Information and Communication Technology
IP	**:**	Internet Protocol
IR	**:**	Institutional Repository
LAN	**:**	Local Area Network
LIBIS	**:**	Library Information System
MIS	**:**	Management Information System
TCP	**:**	Transmission Control Protocol
UPS	**:**	Uninterrupted Power Supply
WAN	**:**	Wide Area Network
WWW	**:**	World Wide Web

Operational Definitions

The following definitions apply to all sections of Policy:

Automation : The technique of making an apparatus, a process, or a system operate automatically.

Breach : Means an information security incident that involves users not using ICT facilities and services in an appropriate and responsible manner.

Electronic Identifier : Means the value that is used in Bayero University electronic systems to uniquely identify an individual. An electronic identifier is an attribute of the electronic identity.

Electronic Identity : Means the set of essential information about an individual that is stored electronically by the University.

Electronic Messaging Services : Means information technologies used to create, send, forward, receive, store, or print electronic messages.

ICT Resources : All of the University Information and Communication Technology (ICT) Resources and facilities **mean** any information resources provided by the University to assist or support teaching, learning, research and administrative activities. This includes, but is not limited to, physical spaces designated for teaching, study or research, all digital and electronic information storage, software and communication media devices, including, but not limited to, telephone, mobile phones, wireless or computer networks, computer workstation equipment including laptops, personal digital assistants, electronic E-mail systems, Internet, Intranet and Extranet.

ICT Resources and services: covers

- All types of ICT facilities owned or leased by the University and ICT services provided by the University
- Computer equipment owned or leased by Users, which are used to connect to the University networks and/or the Internet.

Information security incident means any information security event that disrupts the expected standard operation of ICT services and facilities.

Infrastructure means the physical equipment used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, and also the router, aggregator, repeater, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals and data that are transmitted.

Objectionable material as defined by the Nigeria Censorship Act 2002, including material such as child pornography, incitement to violence, torture, and bestiality.

Operating System(s) : Means the main control program that runs a computer and sets the standard for running application programs. It is the first program loaded when the computer is turned on, and it resides in memory at all times. An operating system is responsible for functions such as memory allocation, managing programs and errors, and directing input and output.

Shibboleth : Shibboleth is a single sign-on (log-in) system for computer networks and the Internet. It allows people to sign in using just one identity to various systems run by federations of different organizations or institutions. The federations are often universities or public service organizations.

Student : Means a person who is admitted to, or enrolled in a unit, course or program of study approved by Bayero University, Kano which leads to, or is capable of leading to award of a diploma or degree from the University.

Use of Electronic Messaging Services : Means to create, send, forward, reply, copy, store, print, or possess electronic messages. For the purpose of this procedure, receipt of an electronic message is excluded from this definition to the extent that the recipient may not have control over the content of the message received.

User(s) : All employees, including casual employees, any person enrolled in an award course of study at the Bayero University, Kano and any person registered to attend short courses, seminars or workshops in any unit of the University as well as all other persons including members of the general public, who have been granted access to, and use of, the University's ICT Resources.

A member of the public accessing Bayero University, Kano web pages from outside the University is not by virtue of that activity alone considered to be a User.

Virus : Means malware software such as computer viruses, worms, Trojan horse and spyware programs.

TABLE OF CONTENTS

1.0 Introduction

The importance of Information and Communication Technologies (ICT) in higher education has been well established. Deployment of ICT improves the effectiveness of education, aids literacy movements, and enhances the scope of education by facilitating mobile learning and inclusive education. The impact of ICT and its potential for education is manifold. In many countries, higher educational institutions (HEIs) have embedded ICT into their curriculum, demonstrating high levels of effective and appropriate ICT use to support teaching and learning across various subject areas. In these countries, ICT has a major impact on the education sector, institutional management, and on teaching and learning methods.

ICT resources remain central to University functions, activities and roles. Therefore, their control and monitoring has to be coordinated for the entire University. Against this background, the Bayero University Kano (BUK) in its vision towards world class excellence has set out this ICT policy as an underlying guideline for proper, efficient and effective support and development of ICT functions within the University, as a means of utilizing the available human and technological resources for teaching, learning, research, community service and sustainable development.

This policy document, therefore, is a necessary guide for developers, users and managers of information and ICT resources on appropriate standards, that conform to recognized International standards and industry best practice for adoption by BUK for the acquisition, development, usage and management of ICT resources to ensure availability and proper use and utilization of ICT in executing BUK functions.

Below is a summary of ICT Services and Systems Policy.

1.1 All users will be lawful, efficient, economical and ethical in their use of the University’s ICT Resources, which are provided to create, preserve, transmit and apply knowledge through teaching, research, creative works and other forms of scholarship.

1.2 It is the University Policy to ensure the availability of all anticipated ICT services and systems at any workplace in the University and for selected services to locations beyond the University through the deployment of Common Network Services.

1.3 It is the University Policy to ensure the availability of all anticipated ICT services and systems at any workplace in the University and for selected services to locations beyond the University through the deployment of Common Network Services.

1.4 It is the University Policy to ensure availability of User-level Data Communication Services such as E-mail, Access-to-Internet and Intranet Services.

1.5 It is the University Policy to advocate the use of office automation in all the offices.

1.6 It is the University Policy to enhance both the efficiency and effectiveness of library operations and services through the deployments of an integrated on- line Library Information System (LIBIS).

1.7 It is the University Policy to enhance and streamline student educational, administrative and managerial processes and to improve academic reporting facilities at central, faculty or departmental level through the implementation of an integrated Academic Records Information System (ARIS).

1.8 It is the University Policy to enhance and streamline financial management processes and reporting facilities at both central and faculty levels through the implementation of an integrated Financial Information System (FINIS).

1.9 It is the University Policy to enhance and streamline the human resource management and administrative processes through the implementation of a Human Resource Information System (HURIS).

1.10 It is the University Policy in the broadest sense to promote the deployments of ICT in all areas of teaching and research.

1.11 It is the University Policy to ensure that all students, academic staff, and non - teaching staff are trained on a continuing basis to equip them with the necessary skills to fully exploit the ICT environment in their different functions.

1.12 It is the University Policy to ensure sustainable management of the University's ICT policy and resources.

1.13 It is the University Policy to ensure the growth and sustainability of its ICT resources.

1.14 It is the University Policy to leverage faculty/department/unit effectiveness so as to enable easier access for coverage of University education by using ICT in instruction teaching, learning and research.

1.15 It is the University Policy to encourage internal capacity for the major information systems in collaboration with other institutions and organizations.

2.0 Common Data Services and Office Automation

2.1 Common Data Services

Data Communication forms an integral and essential part of the University ICT Policy. It must ensure availability, maintainability and sustainability of all anticipated ICT services and systems at any workplace in the University.

It is the Bayero University Policy to give priority to the development, deployment and implementation of Data Communication Services at two different but related levels as follows:

(i) Common Network Infrastructure Services, mainly comprising physical network infrastructure, both fiber optics, WIFI and copper, equipment (switches, routers, servers, etc) and communications protocols; Transmission Control Protocol (TCP) and Internet Protocol (IP), are prerequisites for running FINIS, HURIS, ARIS, LIBIS, and application level communication services, such as e-mail and Internet access.

(ii) User-level Data Communication Services such as email, access to Internet and Intranet Services, which essentially are major "users" of the low-level network services.

2.1.1 Electronic Mail Services

The University shall promote the use of electronic mail services to share information, improve communication, and to exchange ideas.

All official correspondences must be through University-based electronic mail e.g. (name.dept@buk.edu.ng).

Email systems are designed to enhance communication within the University and beyond other institutions and organisations. An electronic mail system consists of the following components:

i. The user's front-end application, providing facilities for creating, addressing, sending, receiving and forwarding messages.
ii. The back-end email server application that forwards messages from the sender to the receiver.
iii. A directory service, the Domain Name Service (DNS), that maintains a database with users and services on the network. Users access this service to locate the addressee and his or her email address.

2.1.2 Access-to-Internet Services

Internet is one of the most valuable communication tools for institutions of higher learning and organisations. It provides access to a wealth of information sources, located on computer systems around the world through the World Wide Web.

2.1.3 Intranet Services

Intranet Services include facilities to design, develop and store information formatted as web pages and make them accessible through the LAN of the institution. Generally both Internet/Intranet services use similar software and hardware technology. Intranet Services may be used for on-line publication of parts of corporate databases, maintained by systems like FINIS, LIBIS, ARIS and HURIS. Also in an academic environment Intranet Services are applied to access course manuals and other study and research documentations.

2.1.4 General User Administration System

The administration of all users' accounts, such as students, employees, visitors and others is a tedious task. In order to accommodate the growing numbers of aforementioned users' at Bayero University there will be one user database for the University common system. For students as an example, names, addresses departments and courses are collected. The information on students is extracted from ARIS while the information on employees is extracted from HURIS.

For the students, this implies that the same account, e-mail-address and user-id can be used for the duration of their program. The account automatically expires when the student is no longer active in ARIS. Similarly, employee accounts will be flagged off by HURIS on expiration of their services.

2.1.5 Access Rights

The University will from time to time, establish access levels, rights, privileges, obligations and sanctions consistent with the University Information Policy, aimed at enabling easy access to corporate data and information needed for the different roles of the University community, while assuring the integrity of such data and information and respecting the privacy of individuals.

2.1.6 ICT Use and Coverage

This policy document applies to all users of the University's ICT Resources.

University's ICT Resources and facilities including, but not limited to: mail, telephones, voice mail, SMS, e-mail, NWNet, University Portal, the Intranet, e-Services, securID, computers, printers, scanners, access labs or other facilities that the University owns, leases or uses under License or by agreement, any off campus computers and associated peripherals and equipment provided for the purpose of University work or associated activities, or any connection to the University's network, or use of any part of the University's network to access other networks.

2.1.6.1 Conditions of Use

Use of the University's ICT Resources is restricted to legitimate University purposes only.

For students this generally implies that academic coursework and research as approved by a supervisor while staff usage will depend on the nature of their work.

The use of University ICT Resources through non-University (including personally

owned) equipment is also subject to this policy.

To assist Users to understand the implications of the above condition the following examples of prohibited and permitted use are provided. These examples are indicative only.

a. The University will not tolerate its ICT Resources being used in a manner that is abusive, discriminatory, harassing, rude, threatening, insulting, obscene or otherwise inappropriate.

   It is illegal to use any ICT Resource to harass, menace, defame libel, belittle or discriminate against any other person within or beyond the University. It is important to understand that in matters of discrimination and harassment it is the ***reasonable perception of the recipient*** and not the intention of the sender that is significant.
   Users may be individually liable if they aid and abet others who discriminate against, harass or vilify colleagues or any member of the public. Users who adversely affect the reputation of another person may be charge for defamation by that aggrieved person.

b. Users must not use the University's ICT Resources to collect, use or disclose personal information in ways that breach the University's Privacy Policy. Users must respect and protect the privacy of others.

c. Users are forbidden to use ICT Resources to access, store or transmit pornographic material of any sort other than with specific written approval from an authorised University Officer for research related purposes.
d. The use of ICT Resources for gambling purposes is forbidden.
e. The University prohibits the use of its ICT resources in a manner that constitutes a violation of copyright. The law permits copying and/or printing only with the permission of the copyright owner, with a few very limited exceptions such as fair use for study or research purposes.

   Accordingly Users must not download and/or store copyright material, post copyright material to University websites, transfer copyright material to others or burn copyright material to CD ROMs or other storage devices using ICT Resources, **unless the copyright material is appropriately licensed.**

   Copyright material includes software, files containing picture images, artistic works, live pictures or graphics, computer games, films and music (including MP3s) and video files.

f. ICT Resources must not be used to cause embarrassment or loss of reputation to the University.

g. The University does not permit the use of its ICT Resources for unauthorised profit making or commercial activities. General staff are referred to the University's Code of Conduct.

h. All Internet content made available on the University's ICT Resources must comply with the University's Policy.

i. Users must not use ICT Resources in inappropriate ways, which are likely to corrupt, damage or destroy data, software or hardware, either belonging to the University or to anyone else, whether inside or outside the network. They may only delete and alter data as required by their authorised University activities

> **Note:** This does not apply to specially authorised University computing staff who may be required to secure, remove or delete data and software, and dispose of obsolete or redundant ICT Resources as part of their ICT Resource management duties.

j. Users must not attempt to repair or interfere with, or add any devices (whether hardware or components) to, any ICT Resource, unless they are authorised and competent to do so. All faults or suspected faults must be reported to either the relevant departmental computer services officer or IT Services Helpdesk.

k. ICT Resources must not be used to distribute unsolicited advertising material from organisations having no connection with the University or involvement in its activities.

l. Users of University issued accounts must identify themselves and not use a false identity.

m. University email lists generated for formal University communications must not be used for other than University business.

n. Unless through a personally paid account, files may only be accessed or downloaded if they are related to work or study. In any case, files may only be downloaded if it is legal to do so and steps have been taken to ensure that the files are free from viruses and other destructive codes.

o. Files may only be attached to email messages if the sender believes they are free from viruses and has taken steps to ensure that they do not contain viruses or other destructive code.

p. Users must not attempt to gain unauthorised access to any computer service. The use of another person's login, password or any other security device (e.g. SecurID, digital signature or biometric identification) is not permitted. Nor must Users exploit any vulnerability in systems or (except authorised staff when checking security of systems as part of their duties) use any technology designed to locate such vulnerabilities or circumvent security and if proven would potentially be considered serious misconduct and accordingly may be dealt with under relevant disciplinary provisions. The matter may also be referred to the police and/or the Independent Commission against Corruption.

q. Users must not use ICT Resources for the purposes of subscribing to and accessing fee based services that are for personal use only, unless the subscription or access is from a personally paid account and the Users personally pay the fees for the services and the services are legal.

r. Users must not facilitate or permit the use of the University's ICT Resources by persons not authorised by the University e.g. Users must not set up a wireless relay base station from their University accounts.

s. Limited minor and incidental personal use may be allowed, but it is a privilege and must not interfere with the operation of ICT resources, burden the University with incremental costs, interfere with the User's employment or other obligations to the University and is subject to compliance with University policies. Users should be aware that personal use of the University's ICT Resources may result in the University holding personal information about the User and/or others which may then be accessed and used by the University to ensure compliance with this, and other policies.

t. It is the Bayero University policy that all staff and students must have University e-mail address.

u. It is a policy to use only Bayero University e-mail by all staff and students as medium of correspondence.

v. It is University policy to assign a web-master, saddle with the responsibility of managing and maintenance of University web-site.

2.1.6.2 Monitoring

(a) Use of ICT Resources is not considered private. Users of ICT Resources should be aware that they do not have the same rights as they would use personally owned equipment through commercial service providers.

(b) The University's electronic communication systems generate detailed logs of all transactions and use. All Users should be aware that the University has the ability to access these records and any backups. In addition, system administrators have the ability to access the content of electronic communications and files sent and stored using the University's equipment.

(c) The University reserves the right to audit regularly and monitor the use of its ICT Resources to ensure compliance with this policy.

(d) The University also reserves the right to look at and copy any information, data or files (including non-University material) created, sent or received by Users using, or while connected to, the University's ICT Resources in the event of a suspected breach of this or other policies.

2.1.6.3 ICT Resources Breach

To ensure consistent and expedient investigation and management of alleged breaches any alleged breach of the Bayero University's ICT legitimate Use Policy, shall be reported to MIS unit who shall record, investigate and act accordingly to this policy.

2.1.7 Management of Breaches

2.1.7.1 Breach Reporting

Any reported information security incident that is considered to be an alleged breach of ICT use policy or procedures will be classified into:

i. Minor breach - as defined in Schedules A and B. (See Appendix)
ii. Major breach - as defined in Schedules A and B. (See Appendix)

a. All breaches are investigated to establish whether a breach was accidental or deliberate.

b. Consistent classification of breaches and recommended disciplinary actions across the University apply. Guides to the applicable response are described in the following Schedules:

i. Breaches by Staff: Schedule A. (See Appendix)
ii. Breaches by Students: Schedule B. (See Appendix)
iii. Example of classification of breaches: Schedule C. (See Appendix)

2.1.7.1 Breach Management Reporting

i. Quarterly management summary reports of breaches are published.
ii. Priorities will be assigned to breaches based on the severity of the impact on the University.
iii. Confidentiality of information related to individual users is maintained at all times.

2.1.8 Breach Penalties

2.1.8.1 Internet Breach

Depending on the type and circumstances of an Internet use breach the following external access restriction penalties will apply:

(a) Password/Account - 20 days
(b) Pornography - 15 days
(c) Copyrighted Content - 15 days
(d) All other - 14 days (after first warning)
(e) Pornography and Copyrighted Content repeat breaches will incur a 15 days external Internet limited access restriction and will be subject to ICT Breach Policy action.
(f) As necessary University network or external Internet access may be suspended.
(g) Depending on the breach history subsequent breaches may result in external

Internet access being fully restricted and escalation to the Divisional Administrator or Head of Department for disciplinary action.

(h) Recovery of unnecessary Internet traffic costs will be considered and sanctioned where appropriate.

2.1.8 .2 Response to Breaches

(a) The University reserves the right to withdraw, restrict or limit any User's access to its ICT Resources if a breach of these conditions is suspected. Any such suspected breach may also be investigated under other University processes, and may result in disciplinary action being taken against the offender in accordance with those processes. This may include a request to reimburse costs (e.g. for unreasonable personal use), disciplinary action (including termination of employment/suspension of candidature) and /or criminal prosecution.

(b) Further the University reserves the right to remove or restrict access to any material within the University domain. Such decisions will be communicated to the appropriate supervisor and account holder.

2.1.9 Security, Confidentiality and Privacy

(a) Matters of a confidential nature should only be conveyed or stored in an electronic format when adequate security measures have been taken.

(b) While the University communications systems are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the protection confidentiality, privacy or security of any information.

(c) Communications on University business in any format or media are official records, subject to statutory record keeping requirements and the University Recordkeeping Policy. This includes email sent and received by staff members on any University related matter. Staff needs to be conscious of the need to preserve official communications in accordance with the relevant University guidelines on the management of electronic records. Care should be taken before deleting any electronic communication that it is not required to be kept as evidence of a decision, authorisation or action.

(d) Sending an email on an official University matter is similar to sending a letter on University letterhead. Such email transactions should be handled with the normal courtesy, prudence and formality of all other University communications. Users should not write anything in an email that they would not sign off in a memorandum.

Any breach of this policy or associated ICT policy will be managed in accordance with the ICT Breach policy.

3.0 ICT Virus

The University will ensure that approved and maintained licensed anti-virus software from known and trusted sources is deployed, where appropriate anti-virus is available, on Information and Communication Technology (ICT) facilities owned or leased by the University and ICT. Disciplinary actions apply, for violation of this policy and/or procedures.

It is the Bayero University Policy to ensure the integrity and minimize the risk of virus infections to University ICT facilities and services.

3.1 Virus Management

The University shall:

(a) Employ virus management measures at appropriate points of the University network.
(b) Implement virus control software and procedures to ensure that all networked computer servers and ICT managed workstations are protected against virus infection.
(c) Immediately disconnect compromised ICT facilities and services from the University network and these will remain disconnected until the infection has been remedied.
(d) Manage mass virus infections/threats through the ICT emergency management process.
(e) Not connect to the University network computer equipment owned or leased by users, without appropriate and maintained anti-virus software
(f) Disconnect from the University network any user owned or leased equipment that does not have appropriate and maintained anti-virus software installed.

4.0 Using Online Plagiarism Detection Software

Academic integrity is an essential component of teaching, learning and research, fundamental to the very nature of universities. The ideas and work of others must be acknowledged rather than claimed as one’s own.

The purpose of this Plagiarism Policy is to outline:

(a) The University’s commitment to high standards of academic integrity
(b) The issues associated with plagiarism and collusion and their effect on student learning
(c) The principles under which preventing, detecting and dealing with cases of plagiarism and collusion and related forms of cheating are managed.

4.1 Scope

This policy applies to all University students and staff involved in academic assessment tasks and scholarly work.

4.2 Guiding principles

4.2.1 Bayero University recognises that confidence in the academic output of their students is vital to ensure the credibility of the students' academic achievements. To this end the University will use the plagiarism detection softwares such as: Turnitin™, Dupli Checker, Copy Leaks, Plagiarisma etc. It is intended that this software will mainly be used as a supportive and constructive tool by both students and staff.

4.2.2 Plagiarism detection services will be used by staff at Bayero University primarily as a supportive teaching tool to enable students to understand the principles of good academic practice in relation to referencing and the use of academic texts in their own original work.

4.2.3 Plagiarism detection services will be used in the detection of poor academic practice and plagiarism.

4.2.4 The use of plagiarism detection services does not imply that plagiarism is suspected in every assignment that is electronically submitted through this process.

4.2.5 The use of plagiarism detection services will not be restricted solely for the purpose of originality checking.

4.3 Policy

4.3.1 Specific consent is given for the University to submit student work to plagiarism detection services through the enrolment process. This consent is listed in the Terms and Conditions of enrolment.

4.3.2 In giving this consent the student is not waiving their right to ownership of their original academic work.

4.3.3 Programme Handbooks will state the use of plagiarism detection services for each specific programme.

4.3.4 Should the University suspect that plagiarism has taken place they reserve the right to submit any assignment into the plagiarism detection services process.

4.3.5 Tolerable percentage originality will be 75% for M. Phil/PhD, 70% for Masters Degrees and 65% for Bachelor's Degrees for all written works.

4.3.6 There shall be a plagiarism checking unit in the University Library that will check and give certifications to submitted works.

4.3.7 Students of the University must submit their write-ups (theses, dissertations, projects, etc.) to the University Library and obtain plagiarism certifications for inclusion before formal submission.

5.0 ICT Password

All University Information and Communication Technology (ICT) facilities and services that are provided by the University shall comply with the minimum standard for passwords contained within this policy. To ensure that appropriate password controls are implemented that address the risk of unauthorised access into the variety of ICT facilities and services at the University. These can only be achieved by establishing a minimum set of password management controls which apply across ICT facilities and services at the University as a baseline requirement. However, ICT facilities and services used to support and manage infrastructure are excluded from this policy.

5.1 Minimum Standard for Password

The minimum standard for password setting and change is:

Length of password	6 Characters Alphanumeric
Number of unsuccessful login attempts before the username is made inaccessible automatically (locked)	5 times
Duration of lockout period	60 minutes
Period after which a password must be changed	30 days (every 1 months) - Users have the ability to change their own passwords at any time
Reusability of old passwords	Users will not be allowed to use a password they used lately within the last 6 months

5.2 Password Management Principles

All Colleges, Faculties, Departments and Units shall ensure that controlled ICT services comply with the following password management principles:

i. Use a minimum of six characters for a password.

ii. Use at least one numeric character in their password.

iii. Have facilities to control the number of failed accesses.

iv. Have time limits for their use.

v. Have management of the reuse of the same password.

vi. Can be turned off on cessation or transfer of users.

vii. Have a secure process for the transmission of new or replacement passwords

viii. Ensure that all passwords used in automated and/or unattended processes are encrypted where possible.

When purchasing new Information and Communication Technology (ICT) facilities and services check whether the items comply with the minimum standards defined in this policy and report any areas of non-compliance to the Director Procurement Unit.

Users issued with a password have a responsibility to change it immediately after he/she:

a. Has been issued with the initial default password.
b. Has used the same password for more than six months.
c. Is advised by the CIT – Information Security or their local ICT Support staff to change it.
d. Has reason to suspect the password has been observed or compromised.
   Users must not:
e. Share the password with anyone.
f. Write the password down in an insecure location.

A breach of this policy will incur disciplinary action by the University (see Appendix, Minor Breach).

6. Office Automation Services

It is the university's policy to advocate automation in all offices.

In this context the term office automation is used for the application of ICT, mostly desk-top computers and other resources to support general office tasks. Major office automation applications include: word processing, electronic mail, spreadsheet processing, document storage and retrieval, desktop publishing as well as access to Internet.

It is the Bayero university policy to as far as possible deploy and use licensed software as a first option to host all office automation.

6.1 End User Skills Development

In an environment where pedagogic, administrative and managerial processes are automated, the necessary skills to utilize the services and or systems to keep them running, develop, deploy and implement them depend often on high-level skills. It is the Bayero University Policy in the broadest sense to promote the deployment and leverage the power of ICT in all areas of education and research.

It is the Bayero University Policy to ensure and require that all students, academic and non academic staff are trained on a continuing basis to equip them with the necessary skills to fully exploit and leverage the power of ICT environment to discharge their official functions.

The following are University policy level requirements:

a. After appointment to any Academic position, Staff are required to undergo a prescribed training in technology- enhanced interactive teaching and learning techniques.

b. It is required that University should have at least one Multi-purpose computer laboratory with 1 computer per 5 students' capacity.

7.0 Information Systems

7.1 Library Information System

In the Bayero University, Kano, information is provided with the advent of technology in a variety of medium and in both close and remote locations. As such the need to manage information efficiently is crucial to teaching, learning and research. Both library staff and library users will require access to reliable bibliographic information and remote databases hosted within and outside the University and want to access these efficiently.

It is the Bayero University, Kano Policy to deploy an ICT-driven system that will efficiently and effectively host library operations and services through the implementation of an integrated on-line Library Information System (LIBIS).

The projected Library Information System will encompass the following functionality:

a. Circulation Control System.
b. Catalogue Maintenance System giving a high quality of bibliographic records in conformity with the standard cataloguing codes.
c. On-line Catalogue Access.
d. Ability to share resources (catalogues) among libraries at different locations.
e. Acquisitions Control, including search of on-line sources of publications, on-line access to book dealers and book publishers and order placement, checking in, query on-order records.
f. Serials Ordering and Control.
g. On-line (through Internet) access from any workplace to Reference and Information Services (indexes, abstracts, etc) in the University library and other universities, libraries, and institutes.
h. Statistical reporting and management information provision.
i. Plagiarism check unit.

7.2 Academic Records Information System

Academic Records Information System (ARIS) is the generic term for the collection of ICT services that are deployed to host student education related administrative and managerial processes.

It is the Bayero University, Kano Policy to enhance and streamline student education related administrative and managerial processes and to improve

academic reporting facilities at both Central, Faculty and Departmental levels through the deployment and implementation of an integrated Academic Records Information System (ARIS).

The ARIS shall integrate and meet the following essential functional requirements:

a. Management of student personal records.
b. Admission of students.
c. Management of student academic performance records and student academic performance analysis.
d. Curricula and course records management (Academic Program Offerings).
e. Class scheduling (time tabling).
f. Space and teaching staff requirements analysis.
g. Students' financial transaction management.
h. Students' health records management.
i. On-line database query and reporting facilities.
j. Alumni records and activities.

7.3 Financial Information System

The financial management function in any organization encompasses a great number of closely related administrative and managerial processes.

It is the Bayero University, Kano Policy to enhance and streamline financial management processes and reporting facilities at Central, Faculty and Departmental levels through the deployment and implementation of an integrated Financial Information System (FINIS).

The following are the integrated and essential functional requirements to be met by the FINIS:

a. Budget preparation, implementation, monitoring, reporting and evaluation. Given the decentralized nature of budgetary management, it is the University policy to make these functions available to faculties.
b. Debt management.
c. Cash management.
d. Foreign aid management.
e. Expenditure management including authorization of expenditures, personnel costs, vendors, awards.
f. Personnel cost administration (payroll).
g. General Ledger.
h. Budget Ledger.
i. Commitment Ledger.
j. Accounts Payable.

k. Account receivable.
l. Fixed assets management.
m. Inventory Control.
n. Cost accounting functions.
o. Financial analysis and (Web technology based) reporting capabilities

7.4 Human Resource Information System

Human resource management entails adequate utilisation of human labour for productivity and attainment of the Bayero University's mission, goals and objectives. In an institution of higher learning, human resources form an integral part of organizational resource, which is scarce, expensive and difficult to sustain. A university spends a greater percentage of its financial resources on personal emoluments as such the university must intensify its efforts on effective management of its employees for optimum returns on its investment in human capacity.

It is the Bayero University, Kano Policy to enhance and streamline the human resource management and administrative processes through the implementation of a Human Resource Information System (HURIS).

A policy element the university has to address at a higher level is the establishment of a guide about the acceptable relative sizes of academic (line function) and administrative (support function) staff. This will also be reflected in the financial outlays for the core versus the support functions in the university.

Essential functional requirements

The HURIS shall incorporate and meet the following essential functional requirements:

a. Establishing a human resource policy.
b. Plan short- and long-term staff requirements.
c. Recruitment of staff.
d. Job evaluation.
e. Training of staff.
f. Salary administration.
g. Pension fund administration.

7.5 High Level Reporting Applications

The University will promote and support the development of high level reporting applications that cut across all the corporate data bases using data mining and/or other approaches.

7.6 Software Development

It is the university policy to encourage whenever the need arises internal capacity and to develop its own software for the major information systems in collaboration with other institutions and organisation.

8. Library ICT Policy

8.1 Introduction

This policy applies subject to the overall university ICT policy. The policy will be applied alongside other BUK ICT related policies. These are:

a. Automation Policy
b. BUK Digital Repository Policy
c. Information Security Policy.
d. Electronic Resources Policy

8.2 Objectives

The overall objective of the library ICT policy is to provide a regulatory environment and framework for the application of ICTs in the delivery of library services. Specific objectives of the policy are:

a. To facilitate optimal utilisation of the available ICT resources
b. To guide the department on proper management of the library ICT resources
c. To provide mechanisms for security of library ICT resources and facilities
d. To give direction in utilisation of ICTs for library service delivery

8.3 Scope

The policy addresses aspects of:

a. The use of the library ICT facilities and resources
b. Management of library ICT facilities and resources

8.4 Guidelines to the use of ICTs and Electronic Resources

8.4.1 Users

The following categories of users are recognized as authorized users of library electronic resources:

a. All members of BUK staff
b. All BUK students .

8.4.2 Online Collections and Services

a. The library will ensure BUK is registered for the use of all subscribed databases
b. The library will market and promote all available e-resources
c. The university community will continually be updated on new resources
d. Links to e-resources will be made available on the library website

e. The library will maintain a database of all electronic resources
f. The library will carry out training on e-resources from time to time
g. Users will be sensitized on implication of using scripts to download articles from subscribed databases.

8.4.3 Management of Passwords

a. A database of passwords needed for the administration of ICT resources will be maintained.
b. Staff will be assigned passwords and rights in line with their work requirements
c. Upon departure, passwords assigned to staff will be disabled
d. Staff will be responsible for passwords assigned to them
e. Users will be sensitized on the need to ensure passwords availed for access to e-resources are not shared with people not authorized to use them.

8.4.4 Digitization

One of the strategic objectives of the library is to preserve and conserve information resources for posterity. Digitization is one aspect of preserving and conserving information resources. Digitization will be guide by the BUK Digital Repository Policy.

8.4.5 Communication

The ICT related channels of communication will be:

a. Library Website Social media (Twitter, Facebook, LinkedIn, YouTube, Flickr, iTunes U, Second Life, Whatsup and MySpace).
a. BUK Official email
b. Any other approved university channels of communication

8.4.6 ICT Human Resources Requirements

The ICT section will consist of:

a. A Systems Librarian
b. An Electronic Resources Librarian
c. A System Administrator
d. ICT Technicians.

8.4.7 Maintenance and repair of Library ICT equipment

The maintenance of the library ICT equipment will be carried out by the University ICT as stipulated by university regulations. The library will liaise with the ICT department for the maintenance and repair of library equipment.

8.4.8 Daily Maintenance

All library staff will be sensitized on the need for proper care and maintenance of the computers in their custody.

8.4.9 Purchase of library ICT equipment

Purchase of ICT related equipment will be guided by the regulations of the University's procurement procedures.

8.4.10 Security of Data

The library will work together with the ICT department to ensure security of all library electronic data. The following guidelines will be followed in ensuring security of data:

a. Back up of data shall be done on a daily basis in the server that is in the library
b. The systems librarian will liaise the library ICT department to ensure there is continuous and consistent back up of library data
c. Staff will be sensitised to consistently back up important information in external disks
d. Administrative passwords will be changed from time to time
e. All computers will be installed with antivirus software to protect them against malicious software

8.4.11 Online Public Access Catalogue (OPAC)

The library will provide terminals for access to the OPAC

8.4.12 Management of Computer Laboratories

a. The library computer laboratories will be open from 8.00am to 10.00pm daily and close during holidays.
b. The library computer laboratories will always be manned when open
c. All users will be required to book for the use of computers in the labs
d. An inventory of ICT equipment will be maintained.

8. 5 Electronic Resources

8.5.1 Introduction

Electronic Resources are materials that require computer intervention in order to access their content and make it useful. The E-resources can be accessed either through a personal computer or handheld mobile device. They may either be accessed remotely via the Internet or locally. Some of the most frequently encountered types are:

a. E-journals
b. E-books
c. Full-text (aggregated) databases

d. Indexing and abstracting databases
e. Reference databases (biographies, dictionaries, directories, encyclopaedias, etc.)
f. Numeric and statistical databases
g. E-images
h. E-audio/visual resources whether through a personal computer or handheld mobile device.

Bayero University in liaison with the Library will make resources available in electronic format wherever it is appropriate to do so, taking into account teaching and research needs, cost effectiveness, technical requirements, user authentication and licensing and preservation issues.

8.5.2 Purchasing

8.52.1 The University seeks to purchase electronic resources within nationally or internationally negotiated agreements.

8.5.2.2 Where these agreements are not available purchase of resources will be on a direct basis with the supplier or, if terms are more favourable, as part of a purchasing consortium

8.5.3 Databases

8.5.3.1 The University will purchase research tools (e.g. bibliographies and reference works) to support its teaching and research needs.

8.5.3.2 Full text databases will be purchased to support teaching and research needs.

8.5.3.3 Databases of multimedia formats (e.g. images, sound and data) will be purchased to support teaching and research needs.

8.5.3.4 Freely available databases, negotiated on behalf of the University will be made available where they support teaching and research needs of the University.

8.5.4 Electronic journals

8.5.4.1 The University follows an "electronic first" policy for the purchase of new journals.

8.5.4.2 Journals will be purchased in print and electronic format (when available) where a title specifically relates to the teaching and research needs of the University

8.5.4.3 Backfiles of e-journals will be purchased when the title is considered essential for the teaching and research needs of the University and when a backfile is available via an approved vendor.

8.5.4.4 E-journal packages will be purchased where they offer better value for money than purchasing single titles, though the content is usually decided by the supplier and is non-negotiable.

8.5.5 E-books

8.5.5.1 Electronic versions of books will be purchased as additional copies for books in high demand where they are available.

Preferences:

8.5.5.2 Purchase from a single vendor – library users only need to learn one interface and rights.

8.5.5.3 One off purchase instead of leasing & associated recurrent costs

8.5.5.4 Vendors who allow printing and downloading with minimal restrictions

8.5.5.5 Electronic versions of reference works will be purchased to support the teaching and research needs of the University.

8.5.5.6 Purchased e-books will be added to the Library catalogue.

8.5.6 Cancellation

8.5.6.1 Usage of e-resources will be monitored and databases with low usage may be cancelled.

8.5.6.2 Price increases and changes of supplier or content may result in cancellation of subscription.

8.5.7 Access to e-resources

8.5.7.1 Where possible, access to e-resources will be negotiated to allow "walk-in" access for all BUK Library members and off-campus access for all students and staff of the University.

8.5.7.2 BUK e-resources users must agree to abide by the terms of use of the various resources made available to them.

8.5.7.3 Computers will be made available to provide access to e-resources for all users in the Library, although printing will not be supported for external users.

8.5.7.4 The University Library will liaise with the CIT to provide access for students and staff in as user-friendly manner as possible, adopting new technologies as appropriate.

8.5.7.5 All new databases will be listed on the Library web-site

8.5.7.8 New resources will be added to resource discovery tools and catalogued as required

8.5.8 Selection criteria

a. The University purchases electronic resources to support its teaching and research needs.

b. Content should be relevant to more than just a few users.

c. Overlap with existing subscriptions should be kept to a minimum. Where there is substantial overlap with other electronic resources the continuation of subscriptions for overlapping electronic resources needs to be justified.
d. There will be minimal requirement for special set up or software installation.
e. Electronic resources should be web based products.
f. Electronic resources can be readily supported by library staff, without the need for a high level of subject knowledge.
g. Site-wide licenses are preferred with no restrictions on number of concurrent users
h. Shibboleth is the preferred method of user authentication.
i. The library expects the vendor to supply designated standard usage statistics on request
j. Availability of funding will limit the purchase of electronic resources, with particular consideration needed when purchasing ongoing subscriptions
k. Free trials of new resources should be coordinated by the E-services team

8.5.9 Collection Development: BUK Institutional Repository Online

a. BUK IR Online is a free, publicly accessible repository of the research outputs of the University.
b. The repository contains both full text papers and metadata only (descriptive) records of research carried out by the students and staff of the University.
c. Full text materials will be made available where copyright allows, otherwise the reference details can be deposited and a link to the online location of the research paper will be included (if available)
d. Library staff manage and maintain the database in liaison with the Director and staff in the Research and Documentation Office.

8.5.10 Off-line Electronic Resources

8.5.10.1 Purpose

The University Library supports the instructional and research programs of the University. Toward this aim, the Library collects or provides access to materials in multiple formats, including electronic formats. The challenges to providing access to off-line electronic resources warrant a separate collection development policy focusing on these materials. This policy will provide guidelines for the selection and acquisition of off-line electronic resources as well as the provision of access. Related collection development documents will address procedural concerns in detail.

8.5.10.2 Scope

This policy seeks to address the selection and acquisition of off-line electronic resources, primarily those monographic titles available on CD-ROM or any other Storing Device. These resources may be:

a. numeric data files
b. textual files
c. bibliographic files
d. graphic and multimedia files
e. courseware/instructional files
f. software needed specifically to utilize resources listed above.

8.5.10.3 Location

The Main Library will be the central location of most of these resources as well as the central access provider. Other libraries and branches, such as: Science, Law, Mambayya House (AKCDS), AKTH Medical College, Agriculture and Engineering Libraries also house and provide access to off-line electronic resources, appropriate for their individual missions.

8.5.10.4 Electronic Resources Accompanying Other Formats

External Storages and CD-ROMs may accompany other formats--monographs, serials, films, videos, or audio recordings. When possible, the Library will purchase and provide access to these materials in compliance with this policy's guidelines. If off-line electronic resources accompany other primary formats, they will be shelved together in the appropriate location.

8.5.10.5 General Selection Principles

8.5.10.5.1 Selection Responsibility:

Responsibility for selecting these materials falls to individual subject specialists and the head of collection development as these materials fall into their regular selecting responsibility. The coordinator for the E-Services as well as library users and other individuals will offer suggestions to appropriate subject specialists or the head of Collection Development.

8.5.10.5.2 Funding:

Ordinarily, the subject content will determine the individual fund. Subject specialists and the head of collection development will determine the appropriate individual funds to use for purchasing off-line electronic resources. As with all other formats, the Library will consider other allocations for those titles deemed major purchases.

8.5.10.5.3 Adherence to Other Collection Development Guidelines:

a. The purchase of off-line electronic resources should follow present collecting policies whether general or subject specific policies. Specifically, their purchase should adhere to the chronological, geographical, language, and date of publication guidelines set forth in general or subject specific policies.

b. As with other materials subject specialists should also:
   i. consider present curriculum and research needs,
   ii. select materials which meet the standards the Library expects of all materials in regard to excellence, comprehensiveness, and authoritativeness, and
   iii. weigh the purchase of a particular title against other possible acquisitions from material budgets.

c. In addition to content, subject specialists should closely consider the criteria listed below when considering the purchase of off-line electronic resources.
   i. the necessary amount of staff time to provide access, training, and assistance
   ii. the improvement or enhancement that the resource will give to existing print materials
   iii. the long-term viability of resources for preservation purposes
   iv. the long-term usability of a resource's data (10 years or more)
   v. the broad accessibility of the resource under present copyright laws and licensing agreements
   vi. the compatibility of the resource with existing hardware about to be purchased or already in the Library and hardware on the University campuses
   vii. the availability and adequacy of documentation
   viii. the currency of the resource's information, if deemed necessary for subject matter
   ix. the user-friendliness of the resource
   x. the ability to network the resource if deemed appropriate
   xi. the replacement policy of the publisher in the event of damage or theft.
   xii. It is particularly important to consult available published reviews of off-line electronic resources before their acquisition. Reviews can outline how well a resource meets specific criteria and can provide further insight regarding the resource's overall quality. Subject specialists should not necessarily exclude a title because it does not meet every individual criterion. However, subject specialists should attempt to select resources that adequately meet as many of the selection criteria as is possible. Because this format increases the complexity of acquisition and access, subject specialists should include the detailed list of pre-order guidelines when ordering off-line electronic resources.

8.5.10.6 Copyright

a. The Library will comply with the existing copyright laws.

b. The Library will also promote copyright compliance among its users and among its staff.

8.5.10.7 Licensing

a. The Library will negotiate and comply with vendor licensing agreements.
b. Subject specialists should include the detailed list of pre-order guidelines and the necessary licensing agreement, when available, with any order for off-line electronic resources prior to ordering the title.

8.5.10.8 Provision of Access

The Library will maximize access to the Library's off-line electronic resources through several means:

a. Cataloging of each resource
b. Necessary storage
c. Provision, maintenance, preparation, and loading of necessary software and hardware
d. Appropriate staff and user support and training
e. Circulation of resources according to IT circulation procedures.

8.5.10.9 Gifts

a. The Library will evaluate and accept gifts of off-line resources that meet the specific format criteria identified herein and that adhere to other collection development guidelines, whether general or subject specific.
b. Gifts of off-line electronic resources should also follow the Library's gifts policy.

8.5.10.10 Replacements

The Library will replace off-line electronic resources using the same criteria for other formats: demand for the resource, cost, and availability from publishers or vendors.

8.5.10.11 Conversion of Outmoded Off-line Electronic Resources

Off-line electronic resources may operate on computer software and hardware that becomes outdated or obsolete while the resource's information remains valuable. In such cases, the Library will attempt to convert or update off-line electronic resources to a useable format. When conversion of outmoded electronic resources is possible, the Library may decide to convert after examining copyright and licensing of the product, demand for the resource, historical significance and uniqueness of the resource (including cost of the conversion), and availability of the information in another format.

8.5.10.12 Duplicates

The Library will purchase duplicate copies of off-line electronic resources when demonstrated need and other restrictions indicate that networking or other options for providing access are not adequate or available. The Library will also purchase duplicates of electronic resources or purchase duplicates of print resources in electronic format when:

a. the resource has significant historical value
b. one format is unstable
c. a cost benefit for purchasing multiple formats exists
d. multiple formats meet the different needs of user groups
e. the archived format of a resource will not operate with current technology.

8.5.10.13 Policy Review

Because of the complex and dynamic nature of providing access to off-line resources, the head of Collection Development, the coordinator E-Resources Services and other librarians will need to review this policy at least every two years.

9. E-learning

9.1 Policy

It is the University Policy to leverage Faculty/Department/Unit effectiveness and enable easier access to and coverage of university education by using ICT in teaching, learning and research.

To support this policy, Bayero University, Kano will:

i. Create organizational (trainer capacity, training management) and technical (practice lab and computer based training tools, self-paced training mode) conditions assuring continuous in- house e-learning training capabilities in the long-term.
ii. Ensure and require that all students and academic staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the Digital Learning Environment (DLE) in their different disciplines.
iii. Develop university wide and global e-learning networks based on academic interests' groups and research collaborations.
iv. Establish the appropriate common DLE infrastructure and software responsive to academic needs through the designated central technological unit.

9.2 E-Learning Goals

The following are the specific University goals and strategies that relate to the integration of ICTs in the teaching and learning processes.

a. Goal 1: To improve the quality of graduates, by utilizing modern instructional materials and methods, including increased use of ICT in teaching and research.
b. Goal 2: To provide greater access to university education, by developing capacity for increased enrolment through non-conventional approaches in teaching and learning i.e. Distance education and virtual university

9.3 User Skills: Policy Drivers

a. All students shall be required to take the prescribed introductory level module(s) as a requirement for e-learning.
b. All academic staff shall be required to demonstrate the prescribed level of competence for content development of e-learning within the DLE.
c. All new staff shall undergo training in education technology techniques with emphasis on e-learning.
d. Each unit shall set up an e-learning laboratory to develop local capacity in development and evaluating appropriate training software.
e. Units shall develop and nurture complimentary methods of teaching and learning to e-learning as a medium of distance learning both within campus and outreach /upcountry centers, in the long term.
f. The trainers shall use an interdisciplinary approach to e-learning.

9.4 Common DLE Infrastructure and Software

It's the university policy to select the appropriate common DLE infrastructure and software responsive to academic needs through the designated management unit. To the extent possible, preference shall be given to open source platforms.

9.5 E-learning Management

It the University Policy to ensure sustainable management of the university's e-learning policy and resources through the creation of appropriate funding, advisory, management and operational organs that will cater for the broad interests of all users.

9.6 High level E-learning Management

A committee, chaired by the Dean, School of Education, shall be responsible for high level direction, management, implementation of the E-learning function. This committee shall also be responsible for establishing the Educational Technology Resource Unit. The other members of the committee shall be the Registrar, the Director MIS, the Dean Faculty of Computer Science & IT, Dean Faculty of Social Science and the Dean Faculty of Management Science.

The University Senate shall have the authority to review the functions and

composition of this committee.
‘

9.7 Educational Technology Resource Function

An Educational Technology Resource Function shall be established, initially based within the Directorate for ICT Support (DICTS) but evolving to an independent unit in the short to medium term, with the mandate of

a. Working as an E-learning Service function.
b. Coordinating e-learning activities.
c. Vetting proposals on e-learning.
d. Monitoring and evaluating e-learning at Bayero University.
e. Promoting e-learning through awareness seminars, workshops etc.

The proposed unit shall consist of people with ICT skills, teaching experience, technical skills, operational skills, and good communication skills.

9.8 Faculty/Unit E-learning Team

Within a unit/Faculty an E- learning team shall be formed. This shall liaise with the Central Resource Unit, ensure implementation of agreed policies in the faculty, and guide the development and implementation of faculty-specific e-learning activities.

10.0 Data Communication Infrastructure

Data communication (DC) systems provide essential links between users of information and sources of information, and form the basis of the network infrastructure.

It is the University policy to develop a University-wide data communication network consisting of the following building blocks:

a. Inter-campus WAN connections between campuses.
b. Network backbone for each campus.
c. Built backbone for each building.
d. Individual LAN identified on the basis of adjacent rooms and/or workplaces and user groups.

By assembling all university general servers (mail, web, administrative, library, etc) into one room (the IT building) should be designed specifically with cooling system, air- filtering, UPS, backup-facilities and physical protection, optimum performance of the servers could be achieved. However, with a high speed backbone, it will not be necessary to place the servers close to the users.

10.1 Network Implementation Policy

A university-wide network infrastructure can only be built over an extensive period of time. For the purpose of planning, management, and resource availability the actual implementation will take place in a phased approach and will be synchronized with the implementation timing of different ICT services and systems as well as with the (expected/required) physical distribution of future clients (users) and servers of each of the services and systems.

It is the university policy to design and implement all network segments under a single project management structure. However, the timing of those components of the infrastructure, which are a prerequisite to particular services or systems, must be synchronized with the implementation process of those services or systems.

10.2 Network Security Policy

The University's ICT Security Policy is the collection of rules by which legitimate users that are given access to the University's information technology and data must adhere to. The main purpose of a security policy is to inform and guide users, staff, visitors and managers of the requirements and their obligations in protecting technology and information assets.

The following are the basic requirements of securing network resources:

a. Ensuring that only authorized individuals have access to information.
b. Preventing unauthorized creation, alteration, or destruction of data.
c. Ensuring that legitimate users are not denied access to information.
d. Ensuring that resources are used in legitimate ways.
e. A visitor should not have access to university classified information

Several characteristics are associated with an effective and feasible ICT security policy:

a. Implementability.
b. Enforceability.
c. Privacy.
d. Access.
e. Accountability.
f. Response.
g. Flexibility.
h. Sustainability
i. Maintainability.

The following measures shall be taken as part of ensuring security:

a. Networks will be built entirely with switches since this nearly eliminates the possibility for users of "snooping" accounts and passwords from the net.
b. All links between switches will be optical fiber.
c. Encrypted communication methods (like ssh instead of telnet, https,) will be used

by all university critical systems (e.g. FINIS, HURIS, ARIS, and so on).

d. Security policy shall be governed by the University Information Policy.

11.0 ICT Management Policy

It the University Policy to ensure sustainable management of the university's ICT policy and resources through the creation of appropriate policy, advisory, management and operational organs that will cater for the broad interests of all users.

It is the University Policy to provide for the growth and financial sustainability of its ICT resources through appropriate funding and operational mechanisms.

11.1 ICT Committee

The ICT Committee shall be responsible for providing a high-level mechanism to:

a. Monitor and control the progress of all activities arising from the implementation of the University's ICT Policy;
b. Allocate resources according to the agreed master plan
c. Budget for the cost of management, operations, maintenance and expansion through the university budget
d. Recommend proposals for cost-recovery and cost-sharing
e. Determine /approve ICT Policy adjustments arising from technology trends or new visions and strategies.
f. The committee has the responsibility for the review and approval of all ICT-related policies.

ICT Committee shall be constituted by the Vice Chancellor, and shall include members nominated from both the management of academic functions (faculties) and the management of administrative and support function of the university. It shall be chaired by a Senior Academic Staff.

12.0 General Information Resource Ownership Policy

12.1 Ownership

For each ICT resource (computer, data communication device, software, network components, and data storage) an "owner" shall be defined. Ownership of specific ICT resources shall be determined by the University's Management. For example: the Bursary Department shall be the owner of the financial database server computer and the financial database.

12.2 Hiring of External Expertise

Owners are allowed to hire certain support services from external professional providers only if cost-effective and if the expertise involved is not (yet) available in the University and cannot be developed by in-house.

12.3 ICT Fee

The University Council shall put in place a ICT fee payable by each student to ensure that ICT services and systems can be expanded and sustained at the level compatible with the University's needs.

13.0 Social Media Policies and Guidelines

13.1 Introduction

Social media refers to a set of online tools that globally supports social interaction among users. Social media has drastically changed the way we communicate and interact – both as individuals and as institutions – and offers opportunities to connect and engage with a range of key stakeholder groups including prospective and current students, staff, donors, alumni, and friends of the University. The adoption of social media has become more innovative in their use in both academic, professional and personal capacities.

Social media are powerful communications tools that have a significant impact on organizational and professional reputations. Because the use of social media may blur the lines between personal voice and institutional voice, Bayero University, Kano has established the following policies to clarify how best to enhance and protect the University, as well as personal and professional reputations, when participating in social media.

Both in professional and institutional roles, employees are expected to follow the same behavioral standards online as they would in the real world. The same laws, professional expectations, and guidelines for interacting with students, parents, patients, alumni, donors, media, and other University constituents apply. Employees are accountable for any institutionally related content they post to social media sites.

13.2 Entities Affected:

This regulation applies to all employees and units of the University.

13.3 Definition

Social media are defined as media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques online. Examples include but are not limited to: LinkedIn, Facebook, Twitter, YouTube, Flickr, iTunes U, Second Life, WhatsApp and MySpace.

13.4 Best Practices

These guidelines apply to individuals posting on behalf of the University or an official University unit, though they may be helpful for anyone posting on social media in any capacity.

a. **Think twice before posting:** Privacy does not exist in the world of social media. Consider what could happen if a post becomes widely known and how that may reflect both on the poster and the University. Search engines can turn up posts q would not say it at a conference or to a member of the media, consider whether you should post it online. If you are unsure about posting something or responding to a comment, ask your supervisor for input or contact the Office of Public Affairs.

b. **Strive for accuracy**: Check your facts before posting them on social media. Review content for grammatical and spelling errors. This is especially important if posting on behalf of the University in any capacity.

c. **Be respectful**: Understand that content contributed to a social media site could encourage comments or discussion of opposing ideas. Responses should be considered carefully in light of how they would reflect on the poster and/or the University and its institutional voice.

d. **Be active**. Social media presences require diligent care and attention. An effective social media site requires regular updates and fresh or engaging content.

e. **Consider your audience and its potential reaction to your content:** Be aware that a presence in the social media world is or easily can be made available to the public at large. This includes prospective students, current students, current employers and colleagues, and peers. Consider this before publishing to ensure the post will not alienate, harm, or provoke any of these groups.

f. **On personal sites, identify your views as your own**: If you identify yourself as a BUK College/School/Faculty/Department/Unit or staff employee online, it should be clear that the views expressed are not necessarily those of the institution.

13.5 Policies for All Social Media Sites

a. Protect institutional confidential and proprietary information.

b. Do not post confidential or proprietary information about the University, its students, employees, or alumni.

c. Employees who share confidential information, do so at the risk of disciplinary action.

d. Adhere to all applicable University regulations, policies, and procedures.

e. Use Social Media in a manner that complies with University regulations, policies, and procedures, including but not limited to:

    i. Governing Regulations

ii. Administrative Regulations
iii. Human Resource Policies and Procedures
iv. Ethical Principles and Code of Conduct
v. Policy Governing Access to and Use of University Information Technology Resources

f. Adhere to copyright and fair use law When posting, be aware of the copyright and intellectual property rights of others and of the University.

g. Do not use University logos or trademarks without permission: Any use of BUK logos, trademarks or other images must have prior approval. Do not use official logos, trademarks, or any other University images or iconography on personal social media sites.

h. Do not use BUK's name to promote a product, cause, or political party or candidate.

i. Do not announce University news. Do not be the first to announce University or departmental news on a social media site unless preapproved by the Office of Public Affairs. The Director of Public Affairs is the official spokesperson for the University.

j. **Institutional Social Media Policies:** If you post on behalf of an official University unit, the following policies apply, in addition to all policies and best practices listed above:

i. Notify the University Departments or University units that have a social media page or would like to start one should contact the Office of Public Affairs to ensure all institutional social media sites coordinate with other University sites and their content.

ii. All institutional pages must have a full-time appointed employee who is identified as being responsible for content. Ideally, this should be the unit head of the department.

iii. Acknowledge who you are If you are representing the University when posting on a social media platform, acknowledge this.

iv. Use approved photos and University logos Your University social media presence must use photos that accurately depict your department or unit, and approved logos for your area of the University. Public Affairs provides approved photos and logos for various areas of the University.

v. Have a plan: Departments should consider their messages, audiences, and goals, as well as a strategy for keeping information on social media sites up-to-date. The Office of Public Affairs can assist and advise you with your social media planning.

vi. Link back to the University: Whenever possible, link back to BUK website. Ideally, posts should be very brief; redirecting a visitor to content that resides within the University Web environment.

vii. When linking to a news article about the University, check first to see whether you can link to a release on BUK Site, the official University bulletin website instead of to an external publication or other media outlet. (http://www.buk.edu.ng/)

viii. Protect the institutional voice: Posts on social media sites should protect the University's institutional voice by remaining professional in tone and in good taste. No individual unit should construe its social media site as representing the University as a whole. Consider this when naming pages or accounts, selecting a profile picture or icon, and selecting content to post. Names, profile images, and posts should all be clearly linked to the particular department or unit rather than to the institution as a whole.

k. **Non-Compliance:** Non-compliance with this policy may result in any or all of the following:

i. Limitation or revocation of individual or unit rights to use or participate in University-related social media;

ii. Removal of posts or social media accounts; or

iii. Corrective or disciplinary actions and sanctions, as defined in the Human Resources Policy and Procedures, Governing Regulations, Administrative and Governing Regulations, Rules of the University Senate, or Code of Student Conduct.

14.0 AMENDMENTS AND REVIEW

The ICT policy shall be amended annually and reviewed in five years. Members of the University community that wish to propose amendments shall write to the ICT Policy Management Committee.

15.0 CONCLUSION

Institutions of higher learning are today critically dependent on the smooth functioning of ICT and its services. A smooth functioning and running ICT can be assured only if establishment, operation and extension of ICT and ICT enabled functions are effected within a framework that takes full cognizance of the institutions overall strategic goals. As technology changes, planning becomes increasingly important in order to avoid incompatibility and inaccessibility. This ICT policy is a guide to actions to be pursued by the University as advantageous or expedient in its bid to optimize ICT development, usage and application in the University. It entails the vision, mission, goal, principles and plans that will guide the activities of all stakeholders.

References

Policy on the use of University Information and Communication Technology Resources (ICT Resources), The University of Sydney Publication (2010).

Information and Communication Technology: ICT Policy Master Plan Phase 2, Makerere University ICT Policy Master Plan Phase 2 (2005 – 2009)

Information and Communication Technology Services Policies and Procedures Curtin University of Technology, Sarawak Campus, Malaysia, March, 2008.

University of Kentucky Regulations; Administrative Regulation 10:4 (5/6/2011).

E-Sources: https://library.uoregon.edu/colldev/cdpolicies/eresources
https://www.soas.ac.uk/library/about/collectiondevpolicy/electronicresourcespolicy/
https://www.uky.edu/regs/sites/www.uky.edu.regs/files/files/ar/AR10-4.pdf

Appendix

Schedule A – Categories of Breach by staff

Minor Breach

Example of Policy Breach	First Breach	Subsequent Breach
Any activity jointly considered by the staff member's Head or nominee and the ICT Director as inconsistent with the staff member's responsibilities	Email warning & recipient acknowledgement Interview optional	Optional notification to Divisional Administrator or Head of Department Staff disciplinary procedure

Major Breach

Example of Policy Breach	Action
Any audio- visual copyright breach e.g. music, films, videos	Staff disciplinary procedure
Use of copyright software outside the University's License provisions	Staff disciplinary procedure
Giving access to Restricted material to a minor/s	Staff disciplinary procedure Anti Corruption Commission or Police to be advised
Viewing, downloading, storing, sending or giving access to Objectionable material	Staff disciplinary procedure Anti Corruption Commission or Police to be advised

Schedule B – Categories of Breach by Students

Minor Breach

Example of Policy Breach	First Breach	Subsequent Breach
Any activity jointly considered by the student's Head of Department or nominee and the ICT Director as inappropriate and irrelevant to the student's academic progress	Email warning & recipient acknowledgement Interview optional	Optional notification to Divisional Administrator Student disciplinary procedure

Schedule C - Example Categorization of Breaches

NOTE:

- Any information security incident where a legal infringement is suspected MUST be dealt with as a Major Breach.
- Schedule C provides a guideline on breach types and breach categories.

• Doing anything dishonest or illegal. E.g. plagiarizing an assignment (i.e. presenting someone else's work as your own).	Major
• Copying or sharing with others software, music or movies without the written permission of the copyright owner. Some examples: o Copying or sharing sound recordings, films, videos, radio and television broadcasts via email, CD or other electronic means. o Making a CD track or movie available via a file-sharing service (e.g. other peer-to-peer services), an FTP service, or a web-site. o Copying a videotape, CD, or DVD onto another videotape, CD, DVD, computer hard disk, or any other storage media. o "Ripping" a music track to a disk or duplicating a music CD. o Copying a computer file containing music or video onto a videotape, CD, DVD, computer hard disk, or any other storage media. o Downloading a CD track or movie from a file-sharing service, a peer- to-peer service, an FTP service, or a web-site. o Storing a file on University equipment that contains illegally copied software, music or video storing of files on a personal piece of equipment, copyrighted software or audio-visual material accessed o Using the Universities Internet service.	Major
• Hacking into, meddling with, or damaging any other computer or service. E.g. trying to "break into" or "crash" another computer on the Internet.	Major
• Using another person's identity or authorisation codes. e.g., using someone else's username or password.	Major
• Possessing, accessing or using any unauthorised hacker tools, whether hardware or software based. e.g. "packet sniffers" and	Major

“password crackers”.	
• Viewing, downloading, storing, sending, or giving access to material deemed as objectionable by the Nigerian Censorship. E.g. materials such as child pornography, incitement to violence, torture, and bestiality.	Major
• Giving a person under the age of eighteen years access to material regarded as restricted by the Nigerian Censorship Act 2002. E.g. materials involving sex, drug misuse or addiction, crime, cruelty, and violence.	Major
• Harassing any person. E.g. sending obscene messages, language, pictures or other materials; issuing threats of bodily harm; contacting a person repeatedly without legitimate reason; disrupting another person's lawful pursuits; and invading another person's privacy.	Major
• Unauthorised use of access accounts and/or passwords	Major
• Theft of any ICT Bayero University hardware and software	Major
• Unauthorised viewing, downloading, storing, sending, distributing or giving access to Restricted material using Northwest University facilities and services e.g. CD- ROM, USB etc	Minor
• Unauthorised use of peer-to-peer software	Minor
• Obstruct other student’s from using computers in a Curtin student computer laboratory. E.g. by using it for anything other than academic and research activities.	Minor
• The use of Bayero University facilities and services for the playing of games or chat sessions not associated with the teaching, learning, research or administrative functions of the University.	Minor

ICT Breaches are not necessarily limited to those outlined above.