- **ICT POLICY**

Table of Contents

ACRONYMS **6**

ICT POLICY **7**

1.0 PURPOSE AND SCOPE **7**

1.1 PURPOSE 7
1.2 SCOPE 8
1.3 TERMS USAGE 8

2.0 ICT MANAGEMENT **9**

2.1 ICT SERVICES DEPARTMENT 9
2.2 ICT COMMITTEES 10
2.3 FIRST LEVEL SUPPORT AND LAB ASSISTANTS 10
2.4 USER SUPPORT CENTER 10
2.5 AMENDMENTS TO POLICY 12

3.0 DATA COMMUNICATION AND NETWORKING POLICY **12**

4.0 IT SECURITY AND USAGE POLICIES **13**

4.1 COMPUTER HARDWARE POLICIES 13
4.2 SOFTWARE POLICY 20
4.3 DATA AND INFORMATION POLICY 21

5.0 EMAIL POLICY **23**

5.1 SUBSCRIPTION TO EMAIL FACILITY 23
5.2 EMAIL ADDRESS NAMING CONVENTION AND ACCOUNT TYPES 24
5.3 EMAIL POLICY GUIDELINES 26

6.0 INTERNET POLICY **31**

6.1 MONITORING AND CONTROL 31
6.2 DISCLAIMER OF LIABILITY FOR USE OF THE INTERNET 31
6.3 DOWNLOADING 32
6.4 E-COMMERCE 32
6.5 CHAT AND NEWSGROUPS 33

7.0 WEBSITE POLICY **33**

7.1 WEBSITE GOVERNANCE 33
7.2 WEBSITE STRUCTURE AND CONTENT 34
7.3 WEBSITE RULES AND REGULATION 35

8.0 GENERAL GUIDELINES FOR CREATING WEB PAGES **37**

9.0 ENFORCEMENT OF WEBSITE POLICY **38**

10.0 IT PROCUREMENT GUIDELINES **38**

10.1 SERVICE CONTRACT 39
10.2 TECHNOLOGY ACQUISITION GUIDELINES 39

11.0 IT PROJECT MANAGEMENT GUIDELINES 40
11.1 PROJECT IMPLEMENTATION TEAM 40
12.0 POLICY ENFORCEMENT 41
13.0 CAPACITY BUILDING 41
13.1 INTRODUCTION 41
13.2 SCOPE 41
13.3 POLICY OBJECTIVES 41
OPEN DISTANCE AND E-LEARNING POLICY 45
1.0 INTRODUCTION 45
2.0 DEFINITIONS 45
3.0 CONTEXT AND PROBLEM STATEMENT 46
4.0 JUSTIFICATION 46
4.0 GOAL 47
5.0 OBJECTIVES 47
6.0 LEGAL FRAMEWORK 47
7.0 STRATEGIES 47
7.1 STRATEGY 1: E-LEARNING PLATFORMS (SOFTWARE) MANAGEMENT 47
7.2 STRATEGY 2: E-LEARNING INFRASTRUCTURE MANAGEMENT 48
7.3 STRATEGY 3: E-LEARNING SUPPORT SERVICES 48
7.4 STRATEGY 4: E-LEARNING SECURITY 49
7.5 STRATEGY 5: E-LEARNING DATA MANAGEMENT 49
7.6 STRATEGY 6: REMOTE ACCESS 50
7.7 STRATEGY 7: OPEN DISTANCE CURRICULA DEVELOPMENT 50
7.8 STRATEGY 8: ADMISSION PROCEDURES 51
7.9 STRATEGY 9: OPEN DISTANCE E-LEARNING (ODEL) TEACHING METHODS 51
7.10 STRATEGY 10: OPEN DISTANCE LEARNING (ODL) ASSESSMENT 51
8.0 IMPLEMENTATION FRAMEWORK 51
8.1 INSTITUTIONAL FRAMEWORK 51
8.2 ACTION PLAN 54
9.0 MONITORING AND EVALUATION 56
9.1 ROLE OF THE UNIVERSITY QUALITY ASSURANCE, GENDER AND ICT COMMITTEE 56
10.0 COMMUNICATION OF THE POLICY 57
11.0 INTERPRETATION 57
12.0 COMMENCEMENT AND AMENDMENT 58
13.0 CONCLUSION 58

KING CEASOR UNIVERSITY

ICT POLICY

March 2024

Approval

This policy has been approved on the ...19th... day of ...March.....the year...2024

Signed:

Hon. Dr. Chris Baryomunsi

CHAIRPERSON, KCU COUNCIL

Dr. Charity Basaza Mulenga

VICE-CHANCELLOR

Acronyms

ICTSD	-	ICT Directorate
MIS	-	Management Information System
USC	-	University Steering Committee
PIT	-	Project Implementation Team
KCU	-	King Ceasor University
LAN	-	Local Area Network
DNS	-	Domain Name Services
ICT	-	Information Communication Technology
IP	-	Internet Protocol

ICT POLICY

1.0 Purpose and Scope

1.1 Purpose

This document defines the ICT Policy of King Ceasor University (KCU). The purpose of the KCU ICT Policy is to:

- Provide rules, guidelines and standards to guide users and decision makers in the development and use of ICT Resources.
- Ensure that ICT resources are used efficiently and appropriately in support of teaching, learning, research and administrative functions of the University.
- Ensure that ICT resources are secured and protected against abuse, damage, loss or theft.

This policy shall be publicised through a number of channels. These include:

- ICT training of staff and students
- Orientation Programmes for new staff and students
- The KCU Staff and Student Mailing lists
- New users subscribing to KCU email facility will have an email message about the policy posted to their inbox.
- The University's website (ICT Directorate Web Pages)

The rules in this document are mandatory upon all users of the University's ICT resources. Users are responsible for making themselves familiar with the rules and regulations governing ICT resources and services.

The ICT Directorate (ICTSD) in collaboration with the ICT Advisory Committee and other sub committees that may be formed to manage ICT services in the University is responsible for:

- Publishing, updating, amending the ICT policies to make it relevant to changing times
- Ensuring that users are aware of and acknowledge their responsibility for the safekeeping of all ICT assets in their possession and for providing the necessary policies, tools, guidance and procedures to enable these to be accomplished.

The ICT Policy shall be approved by the University Council in consultation with the University Top management.

1.2 Scope

This ICT Policy provides the policy framework for:

- Managing ICT services and facilities
- Secured and Acceptable use of ICT facilities
- Use of Internet and Email
- Managing the Website
- IT Procurements and
- IT Project Management

This ICT Policy is NOT a procedure manual for handling or using ICT systems or facilities. *Procedures manuals* should be developed for specific ICT systems by the relevant IT Support units for running and managing such systems. Procedures manuals are detailed guidelines that provide steps for handling the day to-day operation and management of ICT systems.

1.3 Terms Usage

ICT equipment:	Refer to computer hardware, software, networking and communication equipment, devices and tools used to provide ICT Services.
ICT Services:	Refer to: o The provision of Internet, Email, access to MIS and Library information resources and e-learning tools o Telephone services o User support – problem resolution, repairs and maintenance o Training o Advisory Services
Users:	Refer to staff and students of the University who use the university's ICT equipment's. Users also include authorised guests and visitors of the university.

User Departments:	Refer to Schools, Departments and Distance Learning Centres of the University.
IT / ICT	*Information Technology* (IT) and *Information and Communication Technology* (ICT) is used interchangeably in this document to refer to computer, networking and telecommunication technologies.

2.0 ICT Management

ICT services in the University shall be managed by:

- ICT Services Department
- ICT Committees

2.1 ICT Services Department

The ICT Services Department (ICTSD) is mandated to provide leadership in the development, management and use of ICT in the University. The department is responsible for:

- Development and implementation of ICT Policies, ICT Strategies and Standards
- Support of the University's ICT Infrastructure. These covers the management and day-to-day operation of:
    - The Network Operating Centre (Server Room)
    - The University's backbone network that interconnects the local area networks (LANs).
    - Computer Labs
    - Telephone System
    - CCTVs
    - Information Systems (online and offline)
- University Email System
- Providing Internet Access
- Providing the technical support of the University Website
- Design, maintenance of the e-learning Platform
- ICT Training for staff and students
- ICT Advisory Services
- Systems Administration

- ERP Management
- Overseeing the ICT needs of other Departments e.g. Library, Academic Registrar etc
- Research and Development

The ICTSD has oversight responsibly for the Setup, Administration, Troubleshooting and Problem Resolution of PCs, Printers, Servers, Networks and Communications systems.

2.2 ICT Committees

There shall be an ***ICT Advisory Committee*** to oversee and advise on ICT developments and use in the university. The ICT Advisory Committee shall be constituted by the Vice-Chancellor.

Other committees may be created as and when required to assist in managing specific ICT services. The Website Management Committee is one example of such Committees (see section 7).

2.3 First Level Support and Lab Assistants

Intern students and Student Assistants shall be engaged by the ICTSD to complement the efforts of the ICT staff through the provision of first level support services.

Each year, the ICTSD in consultation with the HR shall determine the number of intern students that are to be engaged as first level support at the Departments that require their services. The ICTSD will then submit the request to Management on behalf of the Departments.

The intern will undergo a 2 weeks intensive training by the ICTSD and then dispatched to the Departments to provide first level support.

2.4 User Support Center

A User Support centre will be created within the ICT Department and will be the basis for managing problems and support.

The Procedure for user support procedures shall be established for receiving user problems/requests, trouble ticketing and tracking, problem resolution and escalation.

2.4.1 Objective

The objective of the User Support Center is to provide customer-oriented ICT services to the KCU user community by receiving problem calls, requests and enquiries and arranging to have them resolved or addressed by the appropriate ICT personnel.

2.4.2 Service Availability

The User Support Service shall be available during working hours, Mondays to Fridays, 8: 00am to 5:00 pm

The User Support can be reached either through:

- The University Intercom Phone number (***pending intercom connection***)
- Email: support@KCU.ac.ug

2.4.3 General Guidelines

1. Users shall report problems first to the resident ICT User Support Personnel if any, and subsequently to the ICT Manager, if the problem is unresolved.

2. The User Support Personnel will assign a unique **problem number** for a problem call. The caller will use this number to enquire about the status of the problem when following up.

3. If the problem is not resolved within the expected timeframe, the user may escalate problem to the Director, ICT Directorate by calling or sending email at dict@kcu.ac.ug.

2.4.4 Problem Priority

All effort will be made to attend to problems promptly. However due to possible resource constraints or great number of reported problems, responses shall be based on the **Priority** of the problem. For this purpose, problems shall be classified as follows:

1. **Priority 1 Problems**
   These are problems that will be responded to within a maximum of **4 hours** after the problem has been initially logged. Such problems are characterised by:
   - ❖ A campus wide problem or system failure which prevents the entire University from using critical ICT facilities such as Internet, Email or the MIS.
   - ❖ A problem or system failure which greatly impedes a faculty or department's work
   - ❖ A problem or system failure that does not allow a group of users to work at all.

2. **Priority 2 Problems**

The maximum response time for such problems is **8 hours**. These are problems characterised by:

- ❖ Does not allow any user to work at all.
- ❖ Allow users to work but it takes too long for tasks to be completed

3. Priority 3 Problems

These are problems that are a nuisance to the user but do not interfere with his/her ability to perform day to day functions. The maximum response time for such problems is **12 Hours** after they have been logged.

2.5 Amendments to Policy

An amendment could be a modification of an existing policy guideline or an addition to the Policy.

1. A member of the user community shall write to the ICTSD to propose an amendment to the Policy.

2. The ICTSD shall in consultation with the ICT Advisory Committee study the proposal.

3. If the proposed amendment is found to be meritorious, it shall be forwarded to the Vice-Chancellor for final assent.

3.0 Data Communication and Networking Policy

1. This Policy sets out to achieve a streamlined infrastructure approach that will lead to the centralization of network management through the NOC.

2. The university shall develop, operate and maintain a computing and networking infrastructure as well as software systems to provide the following ICT facilities and services:

   - Office Applications (word-processing, spreadsheet, presentation and database)
   - Internet and Email Services
   - Access to Library Resources
   - Access to MIS

- Access to computer labs and
- Other computing facilities and services as they become available.

3. The Computing and Networking infrastructure and software systems of the university comprise:
   - The *Campus Area Network* that links the networks of schools and departments
   - The *Network Operating Centre* (Server Room) which houses centralised equipment for Internet, Email and Intranet Services
   - The various *Servers* such as the MIS and Library servers that provide information resources to the user community
   - Computer Labs
   - Computers at offices
   - Application software
   - Other ICT-related systems

4. The appropriate use, management and secured operation of ICT facilities are spelt out in the sections which follow.

5. The procurement guidelines spelt out in section 8 of this policy shall guide the procurement of hardware, software and networking systems.

4.0 IT Security and Usage Policies

This section offers the policy guidelines aimed at securing ICT systems from:

- Adverse environmental conditions
- Unauthorised access
- Virus attacks
- Inappropriate handling by IT personnel and users

4.1 Computer Hardware Policies

In this Policy, Computer Hardware in refers to:

- **Computers**: Servers, Desktop Computers, Portable Computers (Laptops, Notebooks),
- **Input and Output Equipmen**t (I/O): Disk storage systems, Printers, Scanners, etc

- **Networks Equipment**: Routers, Switches, Modems, etc
- **Communication Systems**: IP TV, VSAT, PABX, Phones, Cabling Systems, etc.

4.1.1 Environmental Conditions

These are policy guidelines aimed at ensuring that the environment within which the ICT systems operate are protected against inappropriate levels of power, temperature, humidity, fire, dirt, etc.

4.1.1.1 Power

Power supply to computers and accessory equipment must be clean and safe. The labs and computers must have adequate UPS protection. The UPS must have sufficient capacity to provide backup power that, at least lasts for the protected equipment to be powered down, should there be a power outage.

4.1.1.2 Fire

1. Computer Labs and Server Rooms shall be equipped with smoke detectors and fire alarm system.

2. Computer Labs and Server Room shall be equipped with Fire extinguisher(s) which must be tested periodically to determine their effectiveness.

4.1.1.3 Air Conditioning

The server room and computer labs **must have air conditioning systems** that operate during normal working hours. The air conditioning systems should keep the room within the equipment manufacturers' recommended specifications for temperature and humidity throughout the year.

4.1.1.4 Lighting

Adequate lighting must be provided in the Server Room and Computer Labs.

4.1.1.5 Cleaning

1. The server room, computer labs and computers must at all times be clean of dust, dirt, rubbish, food and drink.

2. Eating and drinking are prohibited at labs and server rooms

3. The computers must be clean and free of unnecessary contamination.

4.1.2 Access Control

These are policy guidelines aimed at

- Preventing or minimising unauthorised access to computer systems.
- Preventing or minimising damage, theft or loss of equipment

4.1.2.1 Physical Control

1. Server Rooms and Labs must be adequately secured at the doors and windows with locks and burglar proofs.

2. **For the Server Rooms**:

a. A logbook must be maintained to record entries and departures by IT personnel, visitors and service providers. Details of date, time, personnel/student/staff, purpose, and exit time shall be recorded in the logbook.

3. **For Labs:**

a. Shelves/Cabins shall be provided for safe keeping of student bags; bags must not be allowed into the labs.
b. All students who use the labs must be duly authorised through a registration process.
c. At the end of each day of work, Lab Assistants or IT personnel in charge should check all equipment to ensure that they are intact and in good operating condition.
d. A logbook must be maintained to record incidents, events and problems at the lab.

4. Anyone in possession of the keys to the Server Room or labs is totally responsible for that key.

   These responsibilities include:

- Not handing over the key to anyone else while the key is signed out to them
- Not making copies of the key.

5. **Asset Management**
   a. User Departments shall track their computer systems through the use of an **Asset Register**. The Asset Register may be a notebook but preferably a spreadsheet with the following basic information: *Type of Equipment, Serial Number, Model, Specification, Date Purchased, Location (Room, Office), Cost, Life-Cycle (In Years)*, *Status (operation, faulty or under repairs)*.

   b. The ICTSD shall provide template for the Asset Register and make them available to user departments through the website.

   c. **Asset identification:** All IT Equipment shall be identified by an *asset number* in line with the university's asset naming and identification scheme. The asset number shall be engraved on the equipment casing.

   d. **Equipment Movement Tracking:**
      i) An **equipment movement log book** shall be maintained to track movement of computers. Details should include equipment specifications, name of user, where the equipment is being moved from and to, why it is being moved and the date of removal and replacement. A template shall be provided by the ICTSD through the website.

      ii) Any IT equipment other than the individual's laptop taken off site must have the responsible Officer's authorisation for removal.

      iii) Removal of any IT equipment other than laptops from its normal place of use, e.g. from one lab to the other for any reason, must be authorised by the responsible IT Officer and logged in the equipment movement log book.

6. **Insurance:**
   IT Equipment should be insured as part of assets insured by the University or Department.

7. **Lost or Stolen Equipment**
   Lost or stolen computer equipment must be reported to the Head of Department and the Chief Security Officer.

8. **Careless Handling of Equipment**
   Costs/charges due to damage or otherwise as a result of negligence on the part of users shall be borne by the user in question.

9. **Security breaches** must be reported to Head of Department and the Chief Security Officer. These include but are not limited to: unauthorised entry, doors left open or unlocked, faulty locks, broken window glass, windows left open, etc.

10. **Cabling**: Cabling must be kept tidy and neatly arranged to prevent any work hazards. Cabinets for devices should be used where possible. Cables should also be terminated in all cabinets and labelled for easy identification.

4.1.2.2 Logical Control

User IDs and Passwords

a) Generally, all users of computing and networking facilities must be authorised through the assignment of User IDs and Passwords.

b) All guests and visitors to the University must sign-up for Guest User Accounts. The essential 'dos and don'ts' shall be explained to such visitors and guests, prior to their use of the university's computer facilities.

c) Users are advised not to disclose their personal passwords to anybody. Users are responsible for protecting their personal password and for the consequences of their password being known by others.

d) Users may not sign on to any University system using a user id other than that assigned to them.

e) Users are accountable for all system activities that occur using their user id and password.

f) Initially assigned passwords for any users must be changed upon first login.

g) Good practice with passwords will largely be enforced by the system settings. However, users are advised to follow these guidelines:

i) Passwords must be a minimum of eight characters in length and they should either contain both alphabetic and numeric characters or be a phrase of two or more unrelated words.

ii) If Password change is prompted by the system, please do so when requested to.

iii) Passwords must be changed immediately if the user believes he or she has been compromised or noticed anything unusual.

iv) The standard password protected screen saver must be activated when the PC is left unattended.

v) Users should log off when leaving their PCs for a period of 30 minutes or more.

vi) The PC must always be logged off and switched off before being left overnight unless it is running an overnight process, in which case the screen saver must be activated.

4.1.3 Network Control

a) KCU's networking facilities are intended for teaching, learning, research and administrative support purposes

b) The University network infrastructure shall be secured against:
   i) **Email Spam**: These are unsolicited emails that users receive through the internet.
   ii) **Intruder or Hacker Break-ins**: The University's network like all networks connected to the Internet is susceptible to attacks or intrusion by eternal users.
   iii) **Virus, worms, spyware** which create various dysfunctions in computer systems.

c) To avoid interoperability or poor network connectivity problems, User Departments are advised to contact the ICTSD on before installing or making changes in their Local Area Networks (LANs) as well as workstations.

d) Users or User Departments shall seek clearance from the ICTSD for any third-party network connections to the Internet or any external networks.

4.1.4 Anti-virus Policy

1. All computers in the University must have the University's standard antivirus software installed.

2. The ICTSD shall ensure that the relevant Antivirus is installed on all computers once notified. It is the responsibility of every user to avail their machines for the installation of the antivirus software.

3. The ICTSD will provide automatic updates of the antivirus through the network for computers connected to the network once a first-time installation is done.

4. For computers not connected to the network, the officer in charge at the Department should liaise with the ICTSD to have the updates done regularly.

5. The ICTSD must be notified of the antivirus software removal or change to antivirus software.

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

7. Users should call the attention of the resident IT Support officer immediately for assistance if a virus incident or activity is noticed and cannot be cleaned by the user. The problem should be escalated to the ICT User Support if problem persists.

4.1.5 Troubleshooting, Repairs and Maintenance

1. University's Desktops, Portables (Laptops, Notebooks and PDAs) and Printers that that are assigned to user departments and develop faults may be sent to the ICTSD for repairs and maintenance.

2. IT personnel should document and keep system settings up to-date.

3. User Departments may contract an external ICT service provider to maintain such hardware equipment. User Departments shall liaise with the ICTSD to conclude maintenance agreements with external ICT Service Providers.

4. The ICTSD shall provide templates for maintenance contracts and make them available to user departments through the website.

4.1.6 Disaster Recovery and Contingencies

Disaster recovery procedures and contingencies shall be defined and established for mission critical systems such the Internet, Email, MIS systems and Library Information Resources. The objective is to create capacity to restore services within acceptable period of time after a disaster such as major hardware or system failures or failures resulting from fire, flood and earthquakes.

4.1.7 Other User Responsibilities

1. Users shall be responsible for the appropriate use of the facilities provided as specified in this policy, and shall observe conditions and times of usage as published by the University.

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

3. In all cases users should exercise good judgment and take reasonable care to safeguard the equipment, e.g. equipment must be physically secured when not in use and must never be left unattended when not in use.

4. Only university's staff and students are allowed to use the university's ICT facilities. Visitors and guests shall obtain authorisation from the responsible IT officer before use.

4.2 Software Policy

Software refers to both system and application software. The following shall govern the appropriate use of software.

1. **Pirated** or **Unlicensed Software**: No pirated or unlicensed software shall be installed on individual workstations or on servers.

2. **Copying of softwar**e: Users shall not allow KCU licensed software and/or associated documentation, to be copied by outsiders and may not themselves make copies other than those provided for in the relevant licensing agreements.

3. **Application Development Approach:** Standard Software Development Life-Cycle (SDLC) methodology shall be applied to planning, analysis and design, management and implementation of custom-built software.

4. **Software Configurations:** Software configurations should be documented for easier reference.

5. **Game Playing**
   Recreational game playing, that is not part of an authorised and assigned or instructional activity, is not tolerated.

4.3 Data and Information Policy

1. The university will endeavour to protect the confidentiality of information and material furnished by the user and will instruct all computing personnel to protect the confidentiality of such information and material, but the university shall be under no liability in the event of any improper disclosure.

2. Recording or processing information which infringes any patent or breach any copyright must be avoided.

3. All information acquired or created by any user while carrying out the university's business, except that which is specifically exempted as private or personal, is a general university resource. However, each User Department should have individual ownership of its own data resource.

4. **Single Source Principle**: Data should be captured at source to avoid data re-input error and duplication.

5. **Data Accuracy**: Each user should be responsible for the accuracy of the data that they enter into the system and they should own it.

6. Users accept the following specific responsibilities:
   a) ***Security:***
      i) To safeguard their data, personal information and confidential data;

      ii) To take full advantage of file security mechanisms built into the computing systems;

      iii) To follow the security policies and procedures established to control access to and use of data.

   b) ***Confidentiality***:
      i) To respect the privacy of other users; for example, not to intentionally seek or access information on, obtain copies of, or modify data belonging to other users;

      ii) Not to divulge sensitive personal data concerning staff or users to which they have access without explicit authorisation to do so.

      iii) Not to access information and data without proper authority, nor make unauthorised modifications to the contents of any computer system, including deleting or changing data.

      iv) Not to disclose or use computerised personal data for any purpose which contravenes national or international legislation.

7. Data Backups Strategy

   a) A backup strategy and procedures must be established to allow computer systems to recover from effects, which impair availability of and access to system functions and data. The chosen backup strategy must aim to restore services within a specified acceptable period of downtime, driven by KCU business objective, economic and justifiable recovery environment.

   b) In order to ensure prompt and easy recovery from data loss/corruption it is necessary to keep reliable backups of all documents and data.

   c) Both on-site and off-site backups need to be kept.

d) Regularly test the backup media to ensure that the media can be read and can be relied upon for emergency use when necessary.

e) All data backup tapes/CD's/disks must be stored in a secure location (e.g. fireproof safe) and this environment must be conducive to storage of magnetic media. Documents will be archived on a monthly basis.

5.0 Email Policy

The Email facility has been provided to enhance the business of the University through easier, faster communications and interaction among the user community. This policy provides guidance to users to use the facility in an appropriate and beneficial manner.

5.1 Subscription to Email Facility

5.1.1 Subscription by Staff

1. All staff of the university are entitled to an email account.

2. An email address will be created for staff within 2 days, on applying to the ICTSD.

3. Staff may apply by calling the User Support or writing a memo addressed to the ICT Manager, ICTSD. The details required for the email address are: *Name, Department, Category (Senior Member, Senior Staff, Junior Staff) and Contact Phone.*

4. Applicant will be required to change the assigned password on his/her first login.

5.1.2 Student

1. Email Addresses shall be created for Students when they register with the ARs office.

2. Alternatively, students may apply for email address through their respective Departments.

5.1.3 Closure of Staff Email Account

1. The Human Resource Department will notify the ICTSD when a staff leaves the services of the University.

2. The ICTSD will disable the staff account/email address. But before this is done, the ICTSD shall confirm that all official documents and correspondences received through the mailbox of the staff have been printed and filed by the user departments.

3. The staff account/email address will be deleted three months after the staff has left the services of the University.

5.1.4 Closure of Student Email Account

1. Email accounts of all final year students will automatically be deleted one month after completion of course.

2. Students requiring more than one-month retention of email account after completion of course should submit request through their Head of Department.

5.2 Email Address Naming Convention and Account Types

5.2.1 Naming Convention

The University's Email address convention is:

- **Individual Email Address:** *firstnameInitial.lastname@kcu.ac.ug*

  Example: bkomakech@kcu.ac.ug ***(*Komakech Brians**)

  The middle name will be used to differentiate email addresses where two or more users share the same first and last name.

Example: bvkomakech@kcu.ac.ug *(***Komakech Van Brians**)

Where the use of the middle name will still result in duplicate email address names, sequential numbers will be used to differentiate the email address:

For the above example:

Example: *bvkomakech**1**@KCU.ac.ug*

- **Departmental Email Address:** *deptname@kcu.ac.ug*

Example: *ict@kcu.ac.ug (*ICT Services) -

5.2.2 Sub domain Email Accounts

Schools and Departments may request for a sub domain to be created by applying to the ICTSD. An email address with a sub domain will look like: *firstnameInitial.lastname@subdomainName.kcu.ac.ug*

Example: *bkomakech@finance.kcu.ac.ug* (Finance Department)

5.2.3 Department/Special Purpose Email Accounts

Schools, Departments or groups may apply to create a *Departmental/Group* email account to send, receive and store official emails. Special email accounts could be setup for a specific purpose.

Example: *helpdesk@kcu.ac.ug*

5.3 Email Policy Guidelines

5.3.1 Security and Confidentiality

1. The University does not guarantee the confidentiality of electronic mail since it could be intercepted within or outside the university's network.

2. Except as provided elsewhere in this Policy, ICT personnel are not permitted to see or read intentionally, the contents of email messages except where necessary to ensure proper functioning of university email services, or to disclose or otherwise use what they have seen.

5.3.2 Legal Implications

Users should be aware that email has the same standing in law as any other document and that insulting someone in an email may be considered defamatory and may leave the University and/or the individual user open to legal action.

5.3.3 Email Disclaimer

Users may not transmit personal opinions as those of KCU. The following disclaimer will automatically be included as a suffix to all e-mail messages to addresses external to KCU.

E-Mail Disclaimer Sample:

---------- DISCLAIMER ----------

The information contained in this electronic mail transmission is confidential. It may also contain privileged work product or proprietary information. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. If you have received this transmission in error, please disregard it and reply to the sender, then delete it from all directories and destroy all copies of it. Thank you.

5.3.4 Use of Third-Party Email Systems

Third party email systems such as *Hotmail* and *Yahoo* shall be restricted on the university network and it is totally unacceptable for official communication. This policy is aimed at preserving the Internet Bandwidth and safeguarding university data.

5.3.5 Leave, Vacation, Travel

In order to ensure that official information held in a staff's mail box is available when staff takes leave, vacation or travels, the following measures should be taken:

- For staff about to take leave, vacation or travel, the email should be set to automatically inform senders of their *out-of-office status*, with an advice to send the message to an alternative email address if it is official.

- Staff travelling outside or within the country, have the option of setting the email to forward mail messages to an alternative email system where it would be easier to retrieve.

5.3.6 Email Data Backup and Storage Management

1. The size of mailboxes on the email server will be limited by quotas on the server. When a user's mailbox reaches the quota, a message will be displayed requesting the user to clear the mailbox. The user will not be able to send messages, but will be able to receive them.

2. Emails that are 6-months old on the server will be deleted to preserve space on the server.

3. It is the responsibility of the user to backup mails already received in their mailboxes. The central storage email system will hold pending emails for users till they are retrieved by users.

4. The following guidelines are recommended for managing emails:
   a. Save your mails as files on your disk regularly and delete from mail box
   b. Use *departmental mailboxes* to store official emails

c. Adopt the practice of sending copies of official emails to the departmental mailboxes. Such mailboxes should be backed up periodically. Periodically, depending on storage, print email, file, and then purge.

5.3.7 Sending and Receiving Emails

1. **Responsibility**: Users are responsible for e-mail they send and for contacts made.

2. **Composing**: E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.

3. **Carbon copying (cc'ing):** Before carbon copying (cc'ing) anyone, consider whether or not it is necessary for the individual to be receiving the message. E-mail as a medium has increased communication capabilities, but the abuse of copying everyone in the KCU or outside on messages reduces this benefit when users simply delete messages where they are on the 'cc' list as opposed to being directly addressed.

4. **Attachments to e-mail Messages**: Attachment to e-mail messages should be used sensibly. Transmission of large volumes of data in a message can have a drastic effect on the general level of service provided to all other users. If it is necessary to include attachments then these should be restricted to less than 20Mbytes in size when using internal mail, and 10 Mbytes in size when sending to any Internet addresses. Files larger than recommended above should be broken into separate "chunks" (usually zipped) and then transmitted as separate e-mail messages.

5. Attachments are sources of virus attacks. Users should not activate attachments unless they are from a trusted source.

6. The following are forbidden:
   a. Sending of unsolicited bulk mail messages of a personal nature;

   b. Anonymous messages and chain letters must not be sent;

   c. Advertising of personal items;

d. Transmitting any material either as the message or as attachments to a message that is unlawful, obscene, malicious, threatening, abusive, libellous, or hateful, or encourages conduct that would constitute a criminal act or give rise to civil liability or unrest or a breach of the University's policies. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender specific comments, defamatory statements or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.

e. Users are not authorised to retrieve or read any e-mail messages that are not addressed to them. Employee shall not use any password or code, access a file, or retrieve any stored information, unless authorised to do so.

5.3.8 Mailing Lists

Mailing lists shall be created to facilitate communications and dissemination of information in the university. A mailing list may be ***moderated*** or ***non-moderated***. When a list is moderated, messages sent to the list will first be checked by a moderator before it is released to the list members. For a moderated list, messages are sent to the list members without any checks by someone.

For the purpose of this Policy mailing lists are categorised into three types:

- KCU Staff Mailing List
- Student Mailing List
- Other Mailing Lists

5.3.8.1 KCU Staff Mailing List

1. The KCU Staff Mailing List shall be created and used for disseminating university-wide announcements, events and news.

2. The list shall be restricted to staff of the University.

3. All subscribers to the university email system are automatic members of the list.

5.3.8.2 Student Mailing List

1. The Student Mailing List shall be created and used for disseminating university-wide announcements, events and news to students.

2. The list shall be restricted to students of the University.

3. All student subscribers to the university email system are automatic members of the list.

5.3.8.3 Other Mailing Lists

Based on requests from users, the ICTSD shall create on the email server, other mailing lists for Schools, Departments or groups that have some common interest or subject matter to share. For instance a mailing list could be created for senior members of a faculty.

When such lists are created, members of the lists would have to subscribe to the list. In order words it is optional.

Unlike the KCU Staff Mailing list and Student Mailing list, other mailing lists are optional and are restricted to a section or group in the university.

5.3.8.4 Creating a mailing list

1. Applicant will send an email to helpdesk@kcu.ac.ug with the following information:
   - Name of applicant
   - Department
   - Contact Phone
   - Name of List
   - Description of List
   - Whether list will be moderated or not. If moderated the name and email address of the moderator.

2. The mailing list will be created and the applicant notified either by email or phone. This will normally be done within a day by the ICTSD.

6.0 Internet Policy

The Internet facility is primarily provided to enhance learning, teaching, research and administrative functions of the University. The Internet complements the University's library for researching materials and ideas from a variety of sources both national and international.

6.1 Monitoring and Control

1. Since the Internet is an unregulated medium, it is highly subject to abuse. The ICTSD shall regularly inspect internet files held on computers connected to the University's network, to ensure users have not accessed inappropriate sites or sites that have been expressly forbidden.

2. Inappropriate sites will be filtered or blocked to ensure that users do not access their materials. Inappropriate sites are those with materials relating to pornographic, offensive on grounds including but not limited to ethnic origin, religion, politics and gender.

3. Any user who finds a possible abuse as well as security lapse on any system should report the event to the ICTSD.

4. Users who deliberately access inappropriate material or send inappropriate messages to others will also have their Internet access withdrawn and will be dealt with in accordance with University's disciplinary procedures.

6.2 Disclaimer of liability for use of the Internet

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

2. Users are cautioned that some materials from the internet could be offensive and inappropriate.

3. In general, it is difficult to avoid contact with these undesirable materials while using the Internet. Users accessing the Internet do so at their own risk.

4. Users should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is expected.

6.3 Downloading

1. Information that is downloaded from the Internet should be used for official or academic purposes. Copyright laws must be respected and the appropriate credit given to the author or source of the information.

2. Users should be aware that downloading of multimedia-based files slows the network down considerably and will therefore be restricted at peak internet usage times.

3. The downloading of text or images which contain material of an offensive, indecent or obscene nature is prohibited.

4. Any software or files downloaded via the Internet onto the University's computers may be used only in ways that are consistent with their licenses or copyrights.

5. No user may use the University's facilities knowingly to download or distribute illegal software or material.

6. No user may use the University's Internet services to propagate deliberately any virus.

6.4 E-Commerce

1. The use of the University's Internet services to conduct business or e-commerce activities not related to the University is expressly prohibited.

2. The use of the University's Internet services to engage in hacking other sites, accessing unauthorised information within and outside the University; stealing and using credit cards are criminal and prosecutable in the law courts.

6.5 Chat and Newsgroups

1. Users of any chat Internet facilities must identify themselves honestly, accurately and completely when participating in chats or newsgroups.

2. Users may participate in newsgroups or chats in the course of their work or study, but they do so as individuals, speaking only for themselves. Only those users who are duly authorised to speak to the media on behalf of the University may write in the name of the University to any newsgroup or Web site.

3. Internet chat facilities will be highly restricted during peak hours as they are bandwidth intensive.

7.0 Website Policy

7.1 Website Governance

1. **Website Management Committee**: There shall be a Website Management Committee (WMC) that will provide quality assurance on the Content, Look and Feel of the University's Website ensuring that it is in tune with the university's mission, unique identity, core values and status.

   The WMC will be responsible for setting policies governing the nature, content, format, maintenance, timeliness and ownership of information contained on the official pages of the web site.

   The Website Management Committee shall be constituted by the Vice-Chancellor.

2. **ICT Services Department:**
   a. The ICT Services Department (ICTSD) will be responsible for maintaining the content of the Home and main web pages. Information to be put up on these main pages shall be routed through the ICT Office. The ICT officer will have an officer designated as a ***web assistant***. The web assistant will be responsible for updating the website and responding to emails. They will do so with constant consultation of the ICT Services Department.

b. The ICT Services Department will provide technical and advisory support services for the website. The Department will be responsible for maintaining the University's ***web server***.

3. **School and Departmental Website Sub Committees**: Websites of Faculties and Departments that are linked to the University website are required to have a Website Committee to oversee the quality assurance of their website and to ensure that the University's Website Policy is adhered to. There should be a website assistant who will be responsible for updating the Departmental website.

7.2 Website Structure and Content

The web site will be made up of the following web pages:

1. **Main University Web Pages**: These comprise the University Home Page and pages that provide:

    i) The profile of the University i.e., the governance structure, the courses and programmes of the campuses, colleges, schools, faculties, institutes and centres, as well as the administrative departments
    ii) Admission and registration processes and requirements
    iii) University Policies and Regulations
    iv) News, events and announcements.

2. **Departmental Web Pages:** These comprise the pages or website of the respective Schools, Directorates and Centres of the University. These pages provide details of the courses, programmes as well as academic staff. Personal web pages of faculties may be set up under the Departmental websites.

3. **Student Web Porta**l: This will be made up of pages that capture the life, programmes and activities of students.

4. **Affiliates Web Sites:** These are the web sites of the affiliates of the University that the University may choose at its own discretion to have links to.

5. **Others Web site:** These are sites that the university may have links to, for the purpose of collaboration.

7.3 Website Rules and Regulation

7.3.1 Main University Web Pages

1. The ICT Directorate is responsible for updating and maintaining the content of the main university web pages.

2. The content of the main university web pages would reside on the University web server.

7.3.2 Departmental Web Pages

1. By default, where a Department does not have a website, a minimum number of web pages on the University web server shall be allocated to publish information about the Department.

2. The ICT in conjunction with the ICTSD will create a standard set of pages for Department. However, responsibility for maintaining information on the website will rest with the Department's web assistant.

3. Departments may choose to have a web site of their own which may be hosted outside the University's web server. In this case a link will be established on the University's web site to the Department's. Based on the policy provisions in this document, the ICT in consultation with the ICTSD will approve of the establishment of links to departments that have established their own websites.

4. The web pages of department-owned websites should comply with the policy provisions in this document. Websites that do not comply may have their links removed. The decision will be made by the WMC. This regulation applies to Personal pages of faculties.

5. The ICT will ensure that information on all Departments i.e. Schools, Departments, Directorates, Institutes or Centres is available on the website.

7.3.3 Student Web Portal

1. The student web portal will be managed by the Student Guild Representative Council (SGRC) under the auspices of the office of the Dean of Students.

2. The student web portal will be hosted by the University's web server.

3. For other student groups, the decision to link or host pages will be at the discretion of the ICT.

7.3.4 Websites of Affiliates and Others

1. Links to the websites of Institutions affiliated to the University or otherwise would be established at the discretion of the University.

2. The ICT will conduct a due diligence of the institution web site using the provisions in this policy document and grant approval in consultation with the WMC.

7.3.5 Applications to link to the University Website

1. Outside institutions or organisations that wish to establish a link on their website to that of the University's will apply to the ICT.

2. The ICT will conduct a due diligence of the institution and their web site using the provisions in this policy document and grant approval in consultation with the WMC.

7.3.6 General Guidelines for Web Pages

The following guidelines apply to all web pages under the control of the University.

1. **Content Management System**: All web pages or web sites should have a *Content Management System* (CMS) that provides the capability for a web assistant who has no web programming skills to update the information on the web site.

2. **Identification**: All web pages will be identified by the University logo or logotype.

3. **Contact Information:** All web pages will carry the e-mail address of the department or officer responsible for its upkeep. The website assistant will check for e-mail and respond.

4. **Legal Compliance:** All pages may not violate the university's policy and statutes, copyright, libel, obscenity or other local or national laws.

5. **Commercialisation**: Web pages may not be used for commercial uses, sales or money-making ventures except those authorised by the University administration.

6. **Accuracy and Currency**: All pages will be accurate, well-written, concise, and free of spelling and grammatical errors and will otherwise present the University, mission and values in a positive light.

7. **Monitoring**: All pages will be regularly monitored by the web assistants to ascertain that material is current or appropriate. Outdated or inappropriate materials should be removed within five working days when they are noticed.

8.0 General Guidelines for creating web pages

a. The ICT Department will assist departments to create websites and personal pages by providing design templates.

b. All web pages that will be hosted directly by the University's web server will be constructed with PHP/Apache/MySQL platform.

c. The web pages should accommodate cross platforms and operating environment:

d. Network Bandwidth: accommodate low-bandwidth users (dial up modems) and high bandwidth users

e. The web site or pages should be designed taking into consideration the University's mission, image, keeping the site easy to maintain/repair, making the site accessible to those viewers without state-of-the-art Internet access, and striving to make the site accessible to persons with disabilities.

f. Graphics and photographs should be chosen to enhance the informational content of the page. Graphics should be limited in size to no larger than 55 k., with 50 k or less recommended

g. Moving, blinking or flashing objects should be limited.

9.0 Enforcement of Website Policy

a. Any staff, student or individual that notices an error or considers content on the website to be inappropriate may bring it to the attention of the ICT or web assistant in charge of the page.

b. The ICT or web assistant will take measures to address the concern and give a feedback to the complainant.
c. The following will govern the escalation procedures if the issue has far-reaching implications:
    i. Web Assistant of a department will escalate to ICT
    ii. ICT escalates to WMC
    iii. WMC escalates to Academic Board

d. Where an individual who reported a problem on the site is not satisfied, the complaint may be escalated to the WMC.
e. Any page on the University site that violates policy may be removed from the website immediately by the web assistant of the Department or ICT.
f. The WMC will be the final decision-making authority on the University web site.

10.0 IT Procurement Guidelines

The following guidelines are provided for the procurement of IT hardware, software and networking products and services. When in doubt, user departments are to consult the ICTSD for

clarification or advice. ICTSD will publish standards and specifications for computer equipment and software at its website.

10.1 Service Contract

1. User Departments are advised to consult the ICTSD before any contract with any ICT service provider is consummated.

2. The ICTSD will publish Contract Templates that may be adopted for ICT service contracts.

10.2 Technology Acquisition Guidelines

1. **Warranty**: A minimum of 2 years warranty should be specified for all technology acquisitions

2. **Proven Technology**: Only proven hardware and software with available and very well-established support are to be acquired. Preference should be on proven technology, not leading edge

3. **Industry Standards based:** Technologies that conform to international industry standards shall be adopted. This will apply to hardware, networks, operating systems, databases and portable software. Proprietary technology and tools should be avoided where industry standard systems exist.

4. **Compatibility**: New technology components should be compatible with one another and with the existing ICT systems.

5. **Upgradeability and Scalability**: Technology components acquired should be upgradeable or scaleable.

6. **Security:** The Technology component or system must have industry standard security built in.

7. **Desktop and Laptop Computers**: Computers purchased should have sufficient capacity to run applications at satisfactory response time for at least the next 3 years.

11.0 IT Project Management Guidelines

IT Projects are generally risky and should therefore be managed using best Project Management practices.

11.1 Project Implementation Team

1. All IT Projects must have a properly constituted Project Implementation Team (PIT).

2. For a university-wide project, the PIT shall be constituted by the Vice-Chancellor

3. For a Faculty or departmental project, the PIT shall be constituted by the Dean, Director or Head of the Department that is the direct beneficiary of the IT project.

4. The PIT will comprise:
    a. **Project Sponsor** – The Vice-Chancellor, Dean, Director or Head where applicable
    b. Project Manager – Preferably should be appointed from the faculty or department that is the direct beneficiary of the project**.**
    c. **Project Team** - Depending on the nature and scope of the project, the team should be cross-functional (i.e. a mix of Faculty, ICTSD, PMISD, PDMSD, etc)

5. The following shall form the phases of the project:
    a. Project Initiation:
        i. Project Justification and Approval process resulting in an approved budget
        ii. There shall be a **Project Definition Document** that defines at least the goals, objectives, resources to be used, deliverables and time frame of the project
        iii. Identification and selection of Project Team members
        iv. Definition of roles and responsibilities
    b. Project Planning
        i. Preparation of detailed plans for managing the project.
        ii. The planning phase should be used to define the project infrastructure – project filing and documentations and the various procedures for managing the issues, quality, risks, reporting and communications.

c. Project Execution

i. Monitoring and controlling the project plan

ii. Issuing Status Reports

d. Project Closure

i. Formally handing over deliverables and issuing Project Completion report.

12.0 Policy Enforcement

1. The ICTSD in conjunction with the Quality Assurance Directorate, shall audit compliance with this policy from time to time. The outcome of the audit will be a rating of the User Department compliance which shall be published.

2. Users who flout the policy provisions would be sanctioned according to the regulations of the University or the policy sanctions specified in this policy.

13.0 Capacity Building

13.1 Introduction

ICT is constantly evolving, as such, there is need for careful and strategic planning on how to train the implementers to keep pace with the ever-evolving ICT World. It is the responsivity of ICTSD to identify these gaps and strategically plan for appropriate training to address these gaps in the university.

13.2 Scope

This policy applies to all ICT related programs within the University.

13.3 Policy Objectives

The purpose of this policy is to;

- Identity ICT gaps within the university that needs to be addressed
- Plan and implement ICT Training for the improvement of the technical capacity of stakeholders

- Advise management on the best practices in ICT including renumerations, technical training gaps etc

13.4 Policy Delivery

The ICTSD shall

- Develop standard operating procedures (SOPs) for all the computing resources in the university
- Ensure the availability of the necessary resources (hardware/software) for the delivery of the training
- Implement the capacity building with inhouse personnel or hire external subject experts depending on the requirement of the training